Release Notes for Cisco 7000 Family and Cisco 12000 Series Routers for Cisco IOS Release 12.0 S

December 11, 2000

Cisco IOS Release 12.0(14)S

Text Part Number 78-7130-11 Rev. B0

These release notes for Cisco 7000 family and Cisco 12000 series routers support Cisco IOS Release 12.0 S, up to and including Release 12.0(14)S. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents. Cisco IOS Release 12.0 S is based on Cisco IOS Release 12.0 and is tailored for service provider environments. Cisco IOS Release 12.0 S is the follow-on release to Cisco IOS Release 11.1 CC, which was also targeted to the service provider environment. Additionally, many of the features in Cisco IOS Release 12.0 S were first introduced for the Cisco 12000 series routers on Cisco IOS Release 11.2 GS and for the Cisco 7000 family on Cisco IOS Release 12.0 T.

Use these release notes in conjunction with the *Release Notes for Cisco IOS Release 12.0* located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

In addition to the caveats listed in the "Caveats" section, the software caveats that apply to Cisco IOS Release 12.0 also apply to Cisco IOS Release 12.0 S. For information on other caveats that might apply to Cisco IOS Release 12.0 S, the caveats document for Cisco IOS Release 12.0 is located on CCO and on the Documentation CD-ROM.

Contents

CISCO SYSTEMS

Corporate Headquarters: Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco IOS Release 12.0(5)S was the first public release of this software. Many of the features and hardware support in this software have previously been released to customers on other software releases. For information on new features and Cisco IOS commands supported by Release 12.0 S, see the "New and Changed Information" section on page 11 and the "Related Documentation" section on page 105.

System Requirements

Memory Requirements

Tables 1, 2, and 3 list the memory requirements for the platforms supported in Cisco IOS Release 12.0 S.

Table 1 Memory Requirements for the Cisco 7200 Series Platform

Feature Set by Router	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
Service Provider	c7200-p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 56	c7200-k3p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 3DES	c7200-k4p-mz	16 MB	128 MB	RAM

Table 2 Memory Requirements for the Cisco 7500/RSP Series Platform

Feature Set by Router	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
Service Provider	rsp-pv-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 56	rsp-k3pv-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 3DES	rsp-k4pv-mz	16 MB	128 MB	RAM

Table 3 Memory Requirements for the Cisco 12000/GSR Series Platform

Feature Set by Router	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
Service Provider	gsr-p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 56	gsr-k3p-mz	16 MB	128 MB	RAM
Service Provider/ Secured Shell 3DES	gsr-k4p-mz	16 MB	128 MB	RAM

Hardware Supported

Cisco IOS Release 12.0 S supports the following platforms:

- Cisco 7200 series (including the Cisco 7202, Cisco 7204, Cisco 7204 VXR, Cisco 7206, and Cisco 7206 VXR)
- Cisco 7500 series (including the Cisco 7505, Cisco 7507, Cisco 7513, and Cisco 7576)
- Cisco 7000 series routers (including the Cisco 7000 and Cisco 7010) upgraded with the 7000 series Route Switch Processor (RSP7000) and 7000 series Chassis Interface (RSP7000CI)
- Cisco 12000 series (including the Cisco 12008 and 12012)

Determining Your Software Release

To determine the version of Cisco IOS software currently running on Cisco routers, log in to the router and enter the **show version** EXEC command. The following is sample output from the **show version** command. The version number is indicated on the second line.

```
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-P-M), Version 12.0(5)S, RELEASE SOFTWARE
```

Additional command output lines include more information, such as processor revision numbers, memory amounts, hardware IDs, and partition information.

Microcode Software

Table 4 lists the current microcode versions for the Cisco 7500/RSP series. This series includes the Cisco 7000 equipped with the RSP7000 processor, the Cisco 7010 equipped with the RSP7000 processor, and the Cisco 7500 series routers. Note that microcode software images are bundled with the system software image, with the exception of the Channel Interface Processor (CIP) microcode (all system software images) and Versatile Interface Processor (VIP) microcode (certain system software images). Bundling eliminates the need to store separate microcode images. When the router starts, the system software unpacks the microcode software bundle and loads the proper software on all the interface processor boards. VIP and VIP2 microcode is bundled into all Cisco 7500 series feature sets listed in Table 4.

For further information about the CIP microcode, refer to the Cisco document *Channel Interface Processor Microcode Release Note and Microcode Upgrade Instructions*.

Note The Cisco 7000 series previously included the Cisco 7000 and 7010 routers. These products are not supported in Cisco IOS Release 12.0 S. The Cisco 7000 series now includes the Cisco 7000 equipped with the RSP7000 processor and the Cisco 7010 equipped with the RSP7000 processor.

Table 4 Cisco 7500/RSP Series Routers Microcode Versions

Processor or Module	Current Microcode Version	Minimum Version Required
AIP (ATM Interface Processor)	20.18	20.13
CIP/CIP2 (Channel Interface Processor)	26.16	26.2
EIP (Ethernet Interface Processor)	20.6	20.3
FEIP (Fast Ethernet Interface Processor)	20.8	20.7
FIP (FDDI Interface Processor)	20.4	20.4
FSIP (Fast Serial Interface Processor)	20.9	20.9
HIP (HSSI Interface Processor)	20.2	20.2
MIP (MultiChannel Interface Processor)	22.3	22.3
TRIP (Token Ring Interface Processor)	20.2	20.2
VIP2/VIP2C (Versatile Interface Processor)	22.20	22.20

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Caution Cisco IOS images with strong encryption (including, but not limited to, 56-bit data encryption feature sets) are subject to U.S. government export controls and limited distribution. Images to be installed outside the U.S. require an export license. Customer orders may be denied or subject to delay because of United States government regulations. Contact your sales representative or distributor for more information, or send e-mail to export@cisco.com.

Tables 5, 6, and 7 list the newest features and feature sets supported by the Cisco 7200 series, the Cisco 7500/RSP series, and the Cisco 12000 series in Cisco IOS Release 12.0 S and use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS 12.0 S release in which the feature was introduced. Many of these features were initially available on other releases.

Note This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

Table 5 Feature List by Feature Set for the Cisco 7200 Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
ATM PVC Trap Support	(5)	Yes	Yes	Yes
Available Bit Rate Servicing and Virtual Path Shaping on PA-A3 Port Adapters	(5)	Yes	Yes	Yes
BGP Policy Accounting	(9)	Yes	Yes	Yes
Class-Based Quality of Service MIB	(12)	Yes	Yes	Yes
Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers	(14)	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes
Event MIB	(12)	Yes	Yes	Yes
Fast EtherChannel	(8)	Yes	Yes	Yes
Frame Relay Enhancements for K2 Scalability	(5)	Yes	Yes	Yes
Gigabit Ethernet (PA-GE Support)	(7)	Yes	Yes	Yes
Hot Standby Router Protocol MIB	(12)	Yes	Yes	Yes
ifIndex Persistence	(11)	Yes	Yes	Yes
Inverse Multiplexing over ATM Enhancements	(14)	Yes	Yes	Yes
ISL Support	(5)	Yes	Yes	Yes
MPLS over Frame Relay	(10)	Yes	Yes	Yes
MPLS-TE A.List Node Exclusion	(14)	Yes	Yes	Yes
MPLS Traffic Engineering	(5)	Yes	Yes	Yes
MPLS Traffic Engineering OSPF Support	(8)	Yes	Yes	Yes
Multicast BGP	(5)	Yes	Yes	Yes
Multicast Distributed Switching	(5)	Yes	Yes	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol MIB	(12)	Yes	Yes	Yes
Multiport T1/E1 ATM Port Adapters with Inverse Multiplexing over ATM	(11)	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco 7200 Series (continued)

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
Named Community Lists	(10)	Yes	Yes	Yes
New Revision of System Controller Chip for NPE-175/NPE-225	(9)	Yes	Yes	Yes
NPE-175/NPE-225	(6)	Yes	Yes	Yes
NPE-300	(5)	Yes	Yes	Yes
NPE-400	(14)	Yes	Yes	Yes
OC-12c Dynamic Packet Transport (DPT) Port Adapter	(6)	Yes	Yes	Yes
PA-MC-2T3+ Phase-II (T3 Subrate)	(14)	Yes	Yes	Yes
PA-MC-2T3+ Multichannel T3 Port Adapter	(6)	Yes	Yes	Yes
PA-MC-8EI/120, PA-MC-4TI, PA-MC-8TI, and PA-MC-8DSX1 Multichannel E1 and T1 ISDN PRI Port Adapters	(5)	Yes	Yes	Yes
PA-MC-E3 Multichannel E3 Synchronous Serial Port Adapter	(5)	Yes	Yes	Yes
PA-MC-T3 Multichannel T3 Port Adapter	(5)	Yes	Yes	Yes
Secure Shell Client Version 1	(10)	No	Yes	Yes
Secure Shell Version 1	(5)	No	Yes	Yes
Service Assurance Agent	(8)	Yes	Yes	Yes
SNMP Support for Border Gateway Protocol (BGP) Policy Accounting	(10)	Yes	Yes	Yes
SNMP v3	(6)	Yes	Yes	Yes
Tag Switching	(5)	Yes	Yes	Yes
Turbo Access Control Lists (ACLs)	(6)	Yes	Yes	Yes
Two-Port Multichannel DS1/PRI and Multichannel E1/PRI Port Adapters	(7)	Yes	Yes	Yes
VIP-4	(11)	Yes	Yes	Yes
WCCP Enhancements	(11)	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7500/RSP Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
ATM PVC Trap Support	(5)	Yes	Yes	Yes
Available Bit Rate Servicing and Virtual Path Shaping on PA-A3 Port Adapters	(5)	Yes	Yes	Yes
BGP Policy Accounting	(9)	Yes	Yes	Yes
Cisco 7500 Single Line Card Reload	(13)	Yes	Yes	Yes
Cisco 7576 Router	(5)	Yes	Yes	Yes
Class-Based Quality of Service MIB	(12)	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes
Distributed GRE Tunneling Support	(11)	Yes	Yes	Yes
Distributed Multilink Point-to-Point Protocol	(9)	Yes	Yes	Yes
Distributed Traffic Shaping	(7)	Yes	Yes	Yes
Enhanced Gigabit Ethernet Interface Processor	(11)	Yes	Yes	Yes
Event MIB	(12)	Yes	Yes	Yes
Frame Relay Enhancements for K2 Scalability	(5)	Yes	Yes	Yes
Gigabit Ethernet Interface Processor	(5)	Yes	Yes	Yes
Hot Standby Router Protocol MIB	(12)	Yes	Yes	Yes
ifIndex Persistence	(11)	Yes	Yes	Yes
Inverse Multiplexing over ATM Enhancements	(14)	Yes	Yes	Yes
ISL Support	(5)	Yes	Yes	Yes
Low Latency Queueing	(9)	Yes	Yes	Yes
Memory Scan	(6)	Yes	Yes	Yes
MPLS-TE A.List Node Exclusion	(14)	Yes	Yes	Yes
MPLS over Frame Relay	(10)	Yes	Yes	Yes
MPLS Traffic Engineering	(5)	Yes	Yes	Yes
MPLS Traffic Engineering OSPF Support	(8)	Yes	Yes	Yes
Multicast BGP	(5)	Yes	Yes	Yes
Multicast Distributed Switching	(5)	Yes	Yes	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol MIB	(12)	Yes	Yes	Yes

Table 6 Feature List by Feature Set for the Cisco 7500/RSP Series (continued)

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
Multichannel STM-1 Port Adapter for the Cisco 7500 Series Router	(14)	Yes	Yes	Yes
Multiport T1/E1 ATM Port Adapters with Inverse Multiplexing over ATM	(11)	Yes	Yes	Yes
Named Community Lists	(10)	Yes	Yes	Yes
NetFlow Policy Routing	(6)	Yes	Yes	Yes
OC-12c Dynamic Packet Transport (DPT) Port Adapter	(6)	Yes	Yes	Yes
PA-A3 OC-12 ATM Port Adapter	(11)	Yes	Yes	Yes
PA-MC-2T3+ Multichannel T3 Port Adapter	(6)	Yes	Yes	Yes
PA-MC-2T3+ Phase-II (T3 Subrate)	(14)	Yes	Yes	Yes
PA-MC-8EI/120, PA-MC-4TI, PA-MC-8TI, and PA-MC-8DSX1 Multichannel E1 and T1 ISDN PRI Port Adapters	(5)	Yes	Yes	Yes
PA-MC-E3 Multichannel E3 Synchronous Serial Port Adapter	(5)	Yes	Yes	Yes
PA-MC-T3 Multichannel T3 Port Adapter	(5)	Yes	Yes	Yes
Route Switch Processor (RSP8)	(9)	Yes	Yes	Yes
Router-ports Group Management Protocol (RGMP)	(10)	Yes	Yes	Yes
Secure Shell Client Version 1	(10)	No	Yes	Yes
Secure Shell Version 1	(5)	No	Yes	Yes
Service Assurance Agent	(8)	Yes	Yes	Yes
SNMP Support for Border Gateway Protocol (BGP) Policy Accounting	(10)	Yes	Yes	Yes
SNMP v3	(6)	Yes	Yes	Yes
Tag Switching	(5)	Yes	Yes	Yes
Turbo Access Control Lists (ACLs)	(6)	Yes	Yes	Yes
Two-Port Multichannel DS1/PRI and Multichannel E1/PRI Port Adapters	(7)	Yes	Yes	Yes
Versatile Interface Processor-Based Distributed FRF.12	(12)	Yes	Yes	Yes
VIP-4	(11)	Yes	Yes	Yes
WCCP Enhancements	(11)	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 12000 Series

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
1OC-12/STM-4 SRP Line Card	(6)	Yes	Yes	Yes
1OC-48/STM-16 SRP Line Card	(11)	Yes	Yes	Yes
2 x 32-Bit Counters	(10)	Yes	Yes	Yes
3-Port Gigabit Ethernet Line Card	(11)	Yes	Yes	Yes
6-Port Channelized T3-SMB Line Card	(13)	Yes	Yes	Yes
6DS3-SMB Line Card	(6)	Yes	Yes	Yes
8-Port Fast Ethernet Line Card	(6)	Yes	Yes	Yes
8xOC-3 POS or 16xOC-3 POS Line Card	(10)	Yes	Yes	Yes
Access List Performance Improvements for Cisco 12000 Gigabit Switch Routers	(10)	Yes	Yes	Yes
APS Reflector Mode	(8)	Yes	Yes	Yes
ATM PVC Trap Support	(5)	Yes	Yes	Yes
BGP Policy Accounting	(9)	Yes	Yes	Yes
BGP Policy Accounting on 3-Port Gigabit Ethernet Line Cards	(14)	Yes	Yes	Yes
BGP Policy Accounting on Engine 2	(13)	Yes	Yes	Yes
Cisco 12016 Gigabit Switch Router	(8)	Yes	Yes	Yes
Cisco Optical Regenerator	(10)	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes
Enhanced OC-48c/STM-16c Layer 3 Packet-over-SONET Line Card	(7)	Yes	Yes	Yes
Enhanced Quad OC-12c/STM-4c Layer 3 Packet-over-SONET Line Card	(8)	Yes	Yes	Yes
Event MIB	(12)	Yes	Yes	Yes
Extended ACLs on PSA	(14)	Yes	Yes	Yes
Extended Ethernet Frame Size Support	(10)	Yes	Yes	Yes
Frame Relay Switching Diagnostics and Troubleshooting	(12)	Yes	Yes	Yes
Frame Relay Switching on Engine 2	(11)	Yes	Yes	Yes
FRF2.1 Annex 1	(14)	Yes	Yes	Yes
Gigabit Ethernet Line Card	(5)	Yes	Yes	Yes
GRP Redundant Processor Support	(5)	Yes	Yes	Yes
Hot Standby Router Protocol MIB	(12)	Yes	Yes	Yes
ICMP Rate Limiting on Engine 2 POS Line Cards	(14)	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 12000 Series (continued)

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
ifIndex Persistence	(11)	Yes	Yes	Yes
IP Packet Marking	(13)	Yes	Yes	Yes
MPLS Switching Support for Gigabit Ethernet	(7)	Yes	Yes	Yes
MPLS-TE A.List Node Exclusion	(14)	Yes	Yes	Yes
MPLS Traffic Engineering	(5)	Yes	Yes	Yes
MPLS Traffic Engineering OSPF Support	(8)	Yes	Yes	Yes
Multicast BGP	(5)	Yes	Yes	Yes
Multicast Distributed Switching	(5)	Yes	Yes	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes
Multicast Source Discovery Protocol	(5)	Yes	Yes	Yes
Named Community Lists	(10)	Yes	Yes	Yes
NetFlow on GSR	(6)	Yes	Yes	Yes
NetFlow Export Version 5	(14)	Yes	Yes	Yes
NetFlow Support for Gigabit Ethernet	(7)	Yes	Yes	Yes
Per-Interface Rate Control	(11)	Yes	Yes	Yes
Per-VC Queueing	(7)	Yes	Yes	Yes
Policy Routing on Engine 0 and Engine 1	(13)	Yes	Yes	Yes
Process MIB	(6)	Yes	Yes	Yes
Quad OC-12c/STM-4c ATM Line Card	(13)	Yes	Yes	Yes
RFC 1483 Bridged PVC Encapsulation	(5)	Yes	Yes	Yes
Router-ports Group Management Protocol (RGMP)	(10)	Yes	Yes	Yes
Sampled NetFlow on Engine 2 POS Line Cards	(14)	Yes	Yes	Yes
Section Data Communications Channel (SDCC)[1]	(10)	Yes	Yes	Yes
Secure Shell Client Version 1	(10)	No	Yes	Yes
Secure Shell Version 1	(5)	No	Yes	Yes
Service Assurance Agent	(8)	Yes	Yes	Yes
SNMP Support for Border Gateway Protocol (BGP) Policy Accounting	(10)	Yes	Yes	Yes
SNMP v3	(6)	Yes	Yes	Yes
Tag Switching	(5)	Yes	Yes	Yes

Table 7 Feature List by Feature Set for the Cisco 12000 Series (continued)

Features	In	Feature Sets		
		Service Provider	Service Provider/ Secured Shell 56	Service Provider/ Secured Shell 3DES
Turbo Access Control Lists (ACLs)	(6)	Yes	Yes	Yes
Virtual Path Traffic Shaping	(8)	Yes	Yes	Yes
Weighted Random Early Detection (WRED)	(10)	Yes	Yes	Yes

1. SDCC is supported on GSR OC-48-based line cards.

New and Changed Information

New Features in Cisco IOS Release 12.0(14)S

Many of the new features in Cisco IOS Release 12.0 S were introduced in other Cisco IOS releases. For more complete information, refer to the original release.

BGP Policy Accounting on 3-Port Gigabit Ethernet Line Cards

Platforms: Cisco 12000 series

Cisco IOS 12.0 S now supports Border Gateway Protocol (BGP) policy accounting on 3-port Gigabit Ethernet line cards. Please see the “BGP Policy Accounting” section on page 27 for more information about this feature.

Cisco 7200-I/O-GE+E and Cisco 7200-I/O-2FE/E Input/Output Controllers

Platforms: Cisco 7200 series

The Cisco 7200-I/O-GE+E is an Input/Output controller that provides one Gigabit Ethernet and one Ethernet port. It is equipped with a Gigabit Interface Converter (GBIC) receptacle for 1000 Mbps operation and an RJ-45 receptacle for 10 Mbps operation.

The Cisco 7200-I/O-2FE/E is an Input/Output controller that provides two autosensing Ethernet or Fast Ethernet ports and two RJ-45 receptacles for 10/100 Mbps operation.

I/O controllers support the following features:

- Dual EIA/TIA-232 channels for local console and auxiliary ports
- NVRAM for storing the system configuration and environmental monitoring logs
- Two PC card slots that hold Flash disks or Flash memory cards for storing the default Cisco IOS software image
- Flash memory for storing the boot helper image
- Two environmental sensors for monitoring the cooling air as it enters and leaves the chassis

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s14/12s_asio.htm

Extended ACLs on PSA

Platforms: Cisco 12000 series

The Extended ACLs on PSA feature provides 448-Lines Access Control Lists (ACLs) support on the Performance OC-48 line card by implementing the functionality in the Packet Switching ASIC (PSA).

FRF2.1 Annex 1

Platforms: Cisco 12000 series

FRF2.1 Annex 1 for Event Driven Procedures provides a signalling protocol for permanent virtual circuit (PVC) monitoring at the Network-to-Network Interface (NNI) for a frame relay switching network. FRF2.1 Annex 1 generates notification when an event occurs to change status and when an event occurs, it generates immediate notification.

It allows for faster notification of PVC status, such as addition, deletion, or availability, in frame relay switching networks with multiple switching nodes. The faster notification results in better network management as well as increased PVC scalability per interface since LMI procedures are not needed at each NNI node for each PVC in the network.

FRF2.1 Annex 1 adds event driven procedures to the enterprise frame relay network. It enables fast convergence and provides quick responses to any changes within a frame relay network. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s14/fr21anx1.htm

ICMP Rate Limiting on Engine 2 POS Line Cards

Platforms: Cisco 12000 series

The ICMP rate limiting on Engine 2 Packet-over-SONET (POS) line card feature is used to rate-limit ICMP echo-reply traffic in order to protect hosts against Denial of Service (DoS) attacks.

Inverse Multiplexing over ATM Enhancements

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-A3-IMA port adapter has added the following functionalities for Cisco 7500 series routers running Cisco IOS Release 12.0(14)S or later:

- virtual path shaping
- IP-ATM Class of Service mapping on Cisco 7500 series routers (Class-Based Weighted Fair Queueing, Weighted Random Early Detection, Virtual Circuit Bundling)
- the available bit rate (ABR) Quality of Service class

MPLS-TE A.List Node Exclusion

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The MPLS-TE A.List Node Exclusion feature adds the **exclude-address** keyword to the existing **ip explicit-path** command. Multiprotocol Label Switching Traffic Engineering (MPLS TE) now accepts **exclude-address**. If the exclude-address is a flooded MPLS TE link, that link will be excluded from the contraint-based SPF routine. If the exclude-address is a flooded MPLS TE router ID, that entire node will be excluded from the constraint-based shortest path first (SPF) routine.

MPLS TE will only accept all **exclude-address** or all **include-address** when using the **explicit-path** keyword as part of the **tunnel mpls traffic-eng path-option explicit** command.

If the **explicit** keyword identifies an explicit address list that consists of exclude-addresses, that which has been specified will be excluded, and a dynamic constraint-based SPF lookup will be performed.

Multichannel STM-1 Port Adapter for the Cisco 7500 Series Router

Platforms: Cisco 7500 series routers

The PA-MC-STM-1 is a high-speed single-port multichannel STM-1 port adapter. You can configure the PA-MC-STM-1 as a multichannel E1/E0 STM-1 port. The PA-MC-STM-1 can be configured into 63 individual E1 links. Each E1 link can carry a single channel at full or fractional rates, or be broken down into multiple DS0 or Nx64 Kbps rates. The PA-MC-STM-1 supports up to 3 TUG-3/AU-3 transport slots numbered 1 to 3. You can configure each TUG-3/AU-3 to carry 21 SDH TU-12s. Each SDH TU-12 is capable of carrying a channelized E1 frame, which can be to Nx64 Kbps time slots. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s14/12s_stm.htm

NetFlow Export Version 5

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports NetFlow Export version 5 on the Cisco 12000 series GSR. The version 5 export format can be enabled along with traditional NetFlow and Sampled NetFlow features.

The NetFlow Export Version 5 feature provides the ability to export fine granularity data to the NetFlow collector. Per-flow information and statistics are maintained and uploaded to the workstation.

NPE-400

Platforms: Cisco 7200 series

NPE-400 is a new version of network processing engine for Cisco 7200 series routers with the following enhancements:

- RM7000 microprocessor that operates at an internal clock speed of 350 MHz
- Up to 512 MB ECC SDRAM
- 100 MHz SysAD and memory bus speed
- 4 MB Layer 3 cache

The NPE-400 leverages technology from the NPE-225 and NSE-1 to provide a higher performance NPE card.

PA-MC-2T3+ Phase-II (T3 Subrate)

Platforms: Cisco 7200 series, Cisco 7500 series routers

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections. Each T3 interface can now be independently configured to be either channelized or unchannelized. A channelized T3 provides 28 T1 lines multiplexed into the T3. Each T1 line can be configured into one or more serial interface data channels.

Using the **no channelized** command, you can configure the T3 as a single, unchannelized serial interface data channel. You can configure this data channel to use all of the T3 bandwidth or a portion of it. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s14/12s_ct3.htm

Sampled Netflow on Engine 2 POS Line Cards

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports Sampled NetFlow on Engine 2 Packet-over-SONET (POS) line cards.

New Features in Cisco IOS Release 12.0(13)S

Many of the new features in Cisco IOS Release 12.0 S were introduced in other Cisco IOS releases. For more complete information, refer to the original release.

6-Port Channelized T3-SMB Line Card

Platforms: Cisco 12000 series

The 6CT3-SMB line card consists of high-density digital signal level 3 (DS3) service through six copper T3 ports. T3 transmits DS3-formatted data at 44.736 Mbps through the telephone switching network that is used in a digital WAN carrier facility. Each T3 port can carry a full duplex DS3 rate signal. A T3 can be channelized into 28 independent DS1 data channels or up to 35 NxDS0. A total of 168 DS1 channels are supported, or 210 NxDS0 per line card.

The 28 DS1 channels are multiplexed into 7 DS2 channels. The 7 DS2 channels are multiplexed into a single DS3 signal. The6CT3-SMB line card supports further channelization down to the DS0 time slot level (56 or 64 kilobits per second [kbps]).

The 6CT3-SMB line cards perform the High-Level Data Link Control (HDLC) encapsulation and de-encapsulation functions, and all other necessary functions including timing, signaling, and framing in compliance with DS1 and DS3 specifications. The six T3 ports are numbered 0 to 5.

The 6CT3-SMB line card is connected to devices on the remote customer side, using sub-miniature bayonet coupling (SMB) connectors. A single T3 port consists of one SMB connector for receiving (Rx) and one SMB connector for transmitting (Tx).

BGP Policy Accounting on Engine 2

Platforms: Cisco 12000 series

Cisco IOS 12.0 S now supports BGP policy accounting on Engine 2 line cards. Please see the “BGP Policy Accounting” section on page 27 for more information about this feature.

Cisco 7500 Single Line Card Reload

Platforms: Cisco 7500/RSP series

Before the introduction of the Cisco 7500 Single Line Card Reload feature, the only method of correcting a line card hardware failure for one line card on a Cisco 7500 series router required the execution of a Cbus Complex, a process that reloaded every line card on the network backplane. The amount of time taken to complete the Cbus Complex was often inconvenient, and no network traffic could be routed or switched during the Cbus Complex process.

The Cisco 7500 Single Line Card Reload feature allows users to correct a line card hardware failure on a Cisco 7500 series router by reloading the failed line card without reloading any other line cards on the network backplane. During the single line card reload process, all physical lines and routing protocols on the other line cards of the network backplane remain active. Reloading a single line card is also significantly faster than the Cbus Complex execution process.

IP Packet Marking

Platforms: Cisco 12000 series

The IP Packet Marking feature is implemented on the PSA (hardware) and line card CPU (software) on Engine 2 line cards. In the context of this feature, packet marking means setting or changing the 3-bit precedence value in the Type of Service (ToS) field of IP packets that are received on an interface by a user-configured value on the interface. The QoS treatment of the IP packets is then based on the new value of the precedence bits.

Policy Routing on GSR Engine 0 and Engine 1

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports policy routing on Engine 0 and Engine 1 line cards. NetFlow with flow acceleration is currently not supported on GSR.

Quad OC-12c/STM-4c ATM Line Card

Platforms: Cisco 12000 series

The Quad OC-12c/STM-4c ATM line card provides the Cisco 12000 series product line with four 622-Mbps ATM interfaces. The card interfaces to the Cisco 12000 product line's switch fabric and provides four OC-12c/STM-4c SC connectors for duplex single-mode or multimode SONET/SDH connections. There are four ports, numbered 0 to 3, on each line card. Each port has its own set of Status LEDs. Each SONET connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/7193atm.htm

New Features in Cisco IOS Release 12.0(12)S

Many of the new features in Cisco IOS Release 12.0 S were introduced in other Cisco IOS releases. For more complete information, refer to the original release.

Class-Based Quality of Service MIB

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The Class-Based Quality of Service MIB (Class-Based QoS MIB) provides read access to QoS configurations. This MIB also provides QoS statistics information based on the Modular QoS Command Line Interface (CLI), including information regarding class-map and policy-map parameters.

This Class-Based QoS MIB is actually two MIBs: CISCO-CLASS-BASED-QOS-MIB and CISCO-CLASS-BASED-QOS-CAPABILITY-MIB.

To locate MIBs, use the Cisco Network Management Toolkit for MIBs tool on Cisco Connection Online (CCO).

Event MIB

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Event MIB is an asynchronous notification mechanism standardized for use by network management systems using Simple Network Management Protocol (SNMP). The Event MIB provides the ability to monitor MIB objects on a local or remote system using SNMP and to initiate simple actions whenever a trigger condition is met. By allowing notifications based on events, the Network Management Server (NMS) does not need to constantly poll managed devices to find out if something has changed.

Support of the Event MIB has been added to Cisco IOS software to work with network management systems and, when combined with the currently integrated Expression MIB support, provides a flexible and efficient way to monitor complex conditions on network devices.

By allowing SNMP notifications to take place only when a specified condition occurs, Event MIB support reduces the load on affected devices, significantly improving the scalability of network management solutions. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/dtevent.htm

Frame Relay Switching Diagnostics and Troubleshooting

Platforms: Cisco 12000 series

The Frame Relay Switching Diagnostics and Troubleshooting feature enhances Frame Relay switching functionality by providing tools to diagnose problems in switched Frame Relay networks. The **show frame-relay pvc** command has been enhanced to display detailed reasons why packets were dropped from switched permanent virtual circuits (PVCs). The command also displays the local PVC status, the Network-to-Network Interface (NNI) PVC status, and the overall PVC status. If a network problem is observed, the new **debug frame-relay switching** command can be used to display the status of packets on switched PVCs at regular intervals. This new debug command displays information such as the number of packets that were switched, why packets were dropped, and changes in status of physical links and PVCs. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s12/12sfrsdg.htm

Hot Standby Router Protocol MIB

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Cisco IOS Release 12.0(12)S adds support for the Hot Standby Router Protocol (HSRP) MIB for the Cisco 7100 series, 7500 series and 12000 series GSR platforms.

HSRP is a Cisco proprietary protocol defined in RFC# 2281. The HSRP MIB allows network management systems (NMS) to get reports about the “active” or “standby” HSRP status of devices in a network using Simple Network Management Protocol (SNMP) operations. HSRP trap notifications are configured from the Cisco IOS command-line interface (CLI) using the **snmp-server enable traps** command and the **snmp server host** command. A trap notifies the NMS when a router leaves or enters the active or standby state. When an entry is configured from the CLI, the Row Status for that group in the MIB immediately goes to the active state. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s12/12s_hsrp.htm

Multicast Source Discovery Protocol MIB

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The Multicast Source Discovery Protocol (MSDP) MIB feature adds support in Cisco IOS software for the MSDP MIB. This MIB describes objects used for managing MSDP operations using Simple Network Management Protocol (SNMP). Documentation for this MIB exists in the form of an Internet Draft titled "Multicast Source Discovery Protocol MIB" (draft-ietf-msdp-mib-03.txt) and is available through the Internet Engineering Task Force (IETF) at http://www.ietf.org. Refer to the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s12/12s_msdp.htm

Versatile Interface Processor-Based Distributed FRF.12

Platforms: Cisco 7500/RSP series

The Voice over Frame Relay (VoFR) capabilities that were introduced on the Cisco MC3810 multiservice access concentrator beginning with Cisco IOS Release 11.3 were eventually extended to the Cisco 2600 series, 3600 series, and 7200 series router platforms. These capabilities are now available for Cisco 7500 series routers (with a VIP).

When VoFR is configured on a Cisco router, the router is able to carry voice traffic such as telephone calls and faxes over a Frame Relay network.

The Cisco implementation of Voice over Frame Relay provides the following benefits to existing Frame Relay networks:

- Enables real-time, delay-sensitive voice traffic to be carried over slow Frame Relay links.
- Allows dedicated 64-kbps Time-Division Muliplexing (TDM) telephony circuits to be replaced by more economical Frame Relay permanent virtual circuits.
- Allows voice-enabled routers from multiple remote sites to be multiplexed into a central site router through Frame Relay links.
- Utilizes voice compression technology that conforms to ITU-T specifications.
- Enables Cisco 7500 series routers with a VIP to support Frame Relay fragmentation.

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s12/vofr/index.htm

New Features in Cisco IOS Release 12.0(11)S

Many of the new features in Cisco IOS Release 12.0 S were introduced in other Cisco IOS releases. For more complete information, refer to the original release.

1OC-48/STM-16 SRP Line Card

Platforms: Cisco 12000 series

The 1OC-48/STM-16 SRP line card has a pair of OC-48c, fiber-optic standard connector (SC) duplex ports that provide an SC connection for either the single-mode short-reach or single-mode long-reach version.

The 1OC-48/STM-16 SRP line card allows networks to:

- Provide transmit packet priority with 3 separate queues to prevent head-of-line blocking:
  - Control packets are never rate-shaped or back-pressured by the Ring Access Controller (RAC)
  - High-priority packets are rate-shaped by the RAC
  - Low-priority packets are rate-shaped by the RAC
- Priority-map 8 levels IP/SRP into 2 levels of priority (high and low)
  - Software-selectable rate shaping (rate=X or no shaping) for both high- and low-priority data (RAC)
  - Packet priority determined by type of service (ToS) byte in IP Header (RAC + L3)
- Accept or reject a packet from a particular host
- Transmit Spatial Reuse Protocol (SRP) encapsulation at full rate
- Transmogrify an SRP packet into a Packet-over-SONET (POS) packet in order to allow fast path switching in the PSA.
- Transit Path Performance Monitors
  - High/low queue depth (avg, min, max)
  - High/low queue packet delay (avg, min, max)
  - Packet and byte counts by source or destination MAC address
- Receive Path Performance Monitors
  - Packet and byte counts by source or destination MAC address
- Monitors for incoming and outgoing packets in RAC with separate SRP interface counters

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/10567srp.htm#xtocid2983614

3-Port Gigabit Ethernet Line Card

Platforms: Cisco 12000 series

The 3-Port Gigabit Ethernet line card provides Cisco 12000 series routers with three optical Gigabit Ethernet interfaces, which operate faster than 1-Gbps, on a single card. These interfaces are designed to operate as trunks between Cisco 12000 series gigabit switch routers (GSRs) and other routers or Layer 2 switches. These connections are concatenated, and provide for increased efficiency by eliminating the need to partition the bandwidth. The 3-Port Gigabit Ethernet Line card will provide two ports at full line rate provided the third port is shut down. With all three ports turned on, the 3-Port Gigabit Ethernet line card will balance the load across all three ports up to the card packet forwarding limitations of 4 million packets. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/10551ge3.htm

Distributed GRE Tunneling

Platforms: Cisco 7500/RSP series

The Distributed generic routing encapsulation (GRE) Tunneling Support feature allows GRE IP and other features, such as Web Cache Communication Protocol (WCCP) tunneling, to be performed on VIP-based linecards for the Cisco 7500/RSP platform. The tunneling is performed using recursive or “double” switching techniques that are currently deployed on existing non-distributed platforms, the

relevant bits of which are ported into this development. The double switching is performed by handling the received IP packet in the existing code path until it is determined that the packet needs encapsulation or de-encapsulation, at which point the necessary actions are performed, and the resultant IP packet is recursively forwarded through the IP switching path again. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s11/12s_dgre.htm

Enhanced Gigabit Ethernet Interface Processor

Platforms: Cisco 7500/RSP series

The Enhanced Gigabit Ethernet Interface Processor (GEIP+) is a single-port interface processor that, when combined with the appropriate optical fiber cable and a Gigabit Interface Converter (GBIC), provides one Gigabit Ethernet (GE) interface that is compliant with the IEEE 802.3z specification. The GE interface on a GEIP+ operates in full-duplex mode. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7505/vip1/vip4/10699dwg/index.htm

Frame Relay Switching on Engine 2

Platforms: Cisco 12000 series

Cisco IOS Release 12.0(11)S supports Frame Relay switching on Engine 2 for the Cisco 12000 series gigabit switch router (GSR). Frame Relay is an industry-standard, switched data link layer protocol that handles multiple virtual circuits using High-Level Data Link Control (HDLC) encapsulation between connected devices.

ifIndex Persistence

Platforms: Cisco 7200 series, Cisco 750/RSP series, Cisco 12000 series

One of the most commonly used identifiers used in SNMP-based network management applications is the Interface Index (ifIndex) value. IfIndex is a unique identifying number associated with a physical or logical interface; as far as most software is concerned, the ifIndex is the “name” of the interface. Although there is no requirement in the relevant RFCs that the correspondence between particular ifIndex values and their interfaces be maintained across reboots, applications such as device inventory, billing, and fault detection increasingly depend on the maintenance of this correspondence.

Cisco IOS Release 12.0(11)S adds support for an ifIndex value that can persist across reboots, allowing users to avoid the workarounds previously required for consistent interface identification. The Interface Index Persistence feature allows for greater accuracy when collecting and processing network management data by uniquely identifying input and output interfaces for traffic flows and SNMP statistics. Relating each interface to a known entity (such as an ISP customer)allows network management data to be more effectively utilized. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s11/12sifidx.htm

Multiport T1/E1 ATM Port Adapters with Inverse Multiplexing over ATM

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The inverse multiplexing over ATM (IMA) port adapter is a single-width port adapter that allows Cisco 7100 series, Cisco 7200 series, and Cisco 7500 series routers to support inverse multiplexing over ATM. These port adapters allow WAN uplinks at speeds ranging from 1.544 Mbps to 12.288 Mbps for T1 connections and from 2.048 Mbps to 16.384 Mbps for E1 connections.

With this scalable ATM IMA solution from Cisco, network designers and managers can deploy only the bandwidth they need, using multiple T1 or E1 connections instead of more expensive T3 or OC-3 lines to bridge LANs and ATM WAN applications. Enterprises and branch offices can aggregate traffic from multiple lower-bandwidth physical transmission media, such as T1 or E1 pipes, to transmit voice and data at high-bandwidth connection speeds. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe7_1/imatm.htm

PA-A3 OC-12 ATM Port Adapter

Platforms: Cisco 7500/RSP series

The PA-A3 OC-12 is a dual-width ATM port adapter that provides a single-port, 622.08 Mbps connection from Cisco 7500 series routers to any ATM switch. The PA-A3 OC-12 includes two hardware versions (PA-A3-OC12MM and PA-A3-OC12SMI) that support the following standards-based physical interfaces:

- OC-12c/STM-4 multimode
- OC-12c/STM-4 single-mode intermediate reach

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/6228oc12/6228ovrn.htm

Per Interface Rate Control

Per Interface Rate Control (PIRC) controls the input access rate on a single physical interface on the Engine 2 packet-over-SONET (POS) line cards. Examples of this type of line card are the Enhanced OC-48c/STM-16c POS line card and the Enhanced Quad OC-12c/STM-4c POS line card. You can configure PIRC to either set the precedence of a packet and resend it, transmit the packet as-is, or drop the packet.

VIP-4

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The VIP-4 is the fourth generation of Versatile Interface Processors for use with Cisco 7000 series routers using the Cisco 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) and with Cisco 7500 series routers (which also include the Cisco 7507-MX and Cisco 7513-MX routers). The VIP4 installs in the interface processor slots in your Cisco 7000 series or Cisco 7500 series router.

WCCP Enhancements

Platforms: Cisco 7200 series, Cisco 7500/RSP series

WCCP enhancements add support for WCCP Version 2 for Cisco IOS Release 12.0(11)S. The WCCP feature allows you to use Cisco cache engines or third-party cache engines to handle web traffic, reducing transmission costs and downloading time. This traffic includes user requests to view pages and graphics on World Wide Web servers, whether internal or external to your network, and the replies to those requests. When a user requests a page from a Web server (located in the Internet), the router sends the request to a cache engine. If the cache engine has a copy of the requested page in storage, the cache engine sends the user that page. Otherwise, the cache engine retrieves the requested page and the objects on that page from the web server, stores a copy of the page and its objects, and forwards the page and objects to the user.

WCCP transparently redirects a variety of traffic types, specified by protocol (TCP or UDP) and port. Cisco Cache Engines support only redirection of HTTP (TCP port 80) traffic requests from the intended server to a cache engine. End users do not know that the page came from the cache engine rather than the originally requested Web server.

WCCP v2 for Cisco IOS 12.0 S now contains the following new features:

- Distributed CEF Support
- Input Feature
- Flow Acceleration
- Policy Redirection

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s11/index.htm

New Features in Cisco IOS Release 12.0(10)S

Many of the new features in Cisco IOS Release 12.0 S were introduced in other Cisco IOS releases. For more complete information, refer to the original release.

2 x 32-Bit Counters

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports 2 x 32-bit counters. The 2 x 32-bit counters MIB will allow the 64-bit counters ifHCInOctets, ifHCInUcastPkts, ifHCOutOctets, and ifHCOutUcastPkts to each be represented as two 32-bit objects. One object will represent the upper 32-bits and the other the lower 32-bits. The new objects are as follows:

- cHCCounterIfInOctetsUpper
- cHCCounterIfInOctetsLower
- cHCCounterIfInUcastPktsUpper
- cHCCounterIfInUcastPktsLower
- cHCCounterIfOutOctetsUpper
- cHCCounterIfOutOctetsLower
- cHCCounterIfOutUcastPktsUpper
- cHCCounterIfOutUcastPktsLower

8xOC-3 POS or 16xOC-3 POS Line Card

Platforms: Cisco 12000 series

The single-mode or multimode 8xOC-3 POS or 16xOC-3 POS line card allows Cisco 12000 series routers to aggregate large amounts of data on existing fiber networks. The 8xOC-3 POS or 16xOC-3 POS line card interfaces with the switch fabric in the Cisco 12000 series router and provides a support level of 64 ports per 8-port system and 256 ports per 16-port system. Support for quality of service (QoS) packet flow control processing provides an additional value-added routing feature for Internet service providers (ISPs).

The 8xOC-3 POS line card provides Cisco 12000 series routers with 8 OC-3/STM-1 ports per slot or up to 64 OC-3/STM-1 ports per system. The 16xOC-3 POS line card provides Cisco 12000 series routers with 16 OC-3/STM-1 ports per slot or up to 256 OC-3/STM-1 ports per system. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/41812oc3.htm

Access List Performance Improvements for Cisco 12000 Gigabit Switch Routers

Platforms: Cisco 12000 series

Access list (ACL) performance improvements are provided for two types of Cisco 12000 line cards:

- Line cards using engine 1 architecture
- Line cards using engine 2 architecture

The ACL performance improvement is implemented in a slightly different way depending on the line card type. Engine 1 line cards achieve ACLperformance improvement strictly through hardware, using an improved ASIC design. Engine 2 line cards use a microcode enhancement in the packet switch ASIC (PSA) for packet-over-SONET (POS) applications. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s10/hw_acl.htm

Cisco Optical Regenerator

Platforms: Cisco 12000 series

The Cisco Optical Regenerator is a bidirectional OC-48/STM-16 regenerator that sends optical signals over the longest distance possible. It supports single-mode long reach optical-fiber transmission when connected to an OC-48 line card that is installed in a Cisco 12000 series Gigabit Switch Router (GSR). The SONET specification for fiber-optic transmission defines the standard for single-mode fiber. The regenerator provides an end-to-end IP transport for long distances by forwarding SONET/SDH traffic at OC-48 line rates.

The Cisco Optical Regenerator uses only single-mode fiber because signals can travel farthest through single-mode long reach fiber. The maximum distance for single-mode installations of the regenerator is determined by the amount of light loss in the fiber path andby the physical limitation of sending optical fiber to optical light over exceptionally long distances. High-quality single-mode fiber with minimal high-quality splices can carry a Cisco Optical Regenerator signal up to 50 miles (80 kilometers).

Extended Ethernet Frame Size Support

Platforms: Cisco 12000 series

Cisco IOS Release 12.0 S now supports Extended Ethernet Frame Size in accordance with the Network Working Group Internet Draft titled “Extended Ethernet Frame Size Support,” draft-kaplan-isis-ext-eth-00.txt.

MPLS over Frame Relay

Platforms: Cisco 7200 series, Cisco 7500/RSP series

Transmission of Multiprotocol Label Switching (MPLS)-encapsulated packets across a point-to-point Frame Relay subinterface is now supported. Configuration of the feature is identical to configuration of MPLS on any other interface type:

```
(config)# interface Serial1/0.1 point-to-point
(config-if)# tag ip
```

or

```
(config-if)# mpls traffic-engineering tunnels
```

Note that some Frame Relay features (for example, FRF.12 fragmentation) are not supported for MPLS packets.

Named Community Lists

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

With numbered community lists, there are two types of community list numbers (standard and extended), and there can be up to 100 of each of the lists. Named community lists do not have an upper limit on the number of lists that can be defined. The command syntax is as follows:

ip community-list standard [**community-name** | **community-number**] [**permit**|**deny**] **community**

ip community-list extended [**community-name** | **community-number**] [**permit**|**deny**] **regular-expression**

All rules of numbered community lists apply.

Secure Shell Client Version 1

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. Two versions of SSH are available: SSH Version 1, and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The SSH Server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

The SSH Client feature is an application that runs on a reliable TCP/IP transport layer, and provides strong authentication and encryption. The SSH Client in Cisco IOS software allows a user that is running an EXEC session on a Cisco router to log in to another remote Cisco router, and execute commands on the remote router. With authentication and encryption, SSH Client allows for a secure communication over an insecure network. SSH Client Version 1 supports DES and 3DES encryption and userid/password authentication.

Section Data Communications Channel

Platforms: Cisco 12000

On Cisco GSR OC-48 based line cards, Cisco IOS Release 12.0 S now supports the IP/Section Data Communications Channel (SDCC) interface that is available on the Cisco OC-48 Optical Regenerator. To enable this feature, enter the **sdcc enable** command in configuration mode. To disable this feature, enter the **no sdcc enable** command. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/optregen/opt_cfg/regen48.htm

SNMP Support for BGP Policy Accounting

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

BGP Policy Accounting accumulates incoming packet counts and octet counts per interface in the fibidb structure. These counters are now SNMP retrievable because of a new MIB called CISCO-BGP-POLICY-ACCOUNTING-MIB. Each row in the MIB table contains statistics for a particular traffic type on an interface. The table is indexed by ifindex from the IF-MIB and a traffic_index that identifies a particular traffic type. The traffic can be classified into one of eight types using the command-line interface (CLI).

Weighted Random Early Detection

Platforms: Cisco 12000 series

Random Early Detection (RED) is a congestion avoidance mechanism that takes advantage of the TCP congestion control mechanism. By randomly dropping packets prior to periods of high congestion, RED tells the packet source to decrease its transmission rate. Assuming the packet source is using TCP, it will decrease its transmission rate until all the packets reach their destination, indicating that the congestion is cleared.

Weighted RED (WRED) generally drops packets selectively based on IP precedence. Packets with a higher IP precedence are less likely to be dropped than packets with a lower precedence. Thus, higher priority traffic is delivered with a higher probability than lower priority traffic. However, you can also configure WRED to ignore IP precedence when making drop decisions so that nonweighted RED behavior is achieved.

WRED is useful on any output interface where you expect to have congestion. However, WRED is usually used in the core routers of a network, rather than at the edge. Edge routers assign IP precedences to packets as they enter the network. WRED uses these precedences to determine how it treats different types of traffic. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/wred_gs.htm

New Features in Cisco IOS Release 12.0(9)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced in other Cisco IOS releases. For more complete information, refer to the original release.

BGP Policy Accounting

Platforms: Cisco 7200 series; Cisco 7500/RSP series, Cisco 12000 series

BGP Policy Accounting provides a means of charging customers according to the route that their traffic travels. Trans-Pacific, Trans-Atlantic, satellite, domestic, and other provider traffic can be identified and accounted for on a per-customer basis when customers are on a unique software interface. This feature also allows the accounting of traffic to known autonomous system numbers in order to better engineer and plan network circuit peering and transit agreements.

BGP Policy Accounting classifies IP traffic by autonomous system number or autonomous system community string and increments packet and byte counters per input interface. It performs this function using route-maps to classify the traffic into one of eight possible indexes, which represent a traffic classification.

Distributed Multilink Point-to-Point Protocol

Platforms: Cisco 7500/RSP series

The Distributed Multilink Point to Point Protocol (distributed MLP) feature allows T1/E1 lines to be combined in a Versatile Interface Processor (VIP) on a Cisco 7500 series router into a bundle that has the combined bandwidth of multiple T1/E1 lines by using a VIP MLP link. You choose the number of bundles and the number of T1/E1 lines in each bundle, which allows you to increase the bandwidth of your network links beyond that of a single T1/E1 line without the need to purchase a T3 line. Nondistributed MLP can only perform limited links, with CPU utilization quickly reaching 90 percent with only a few T1/E1 lines running MLP. With distributed MLP, you can increase the total capacity of the router. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t3/multippp.htm

Low Latency Queueing

Platforms: Cisco 7500/RSP series

The Low Latency Queueing feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data, such as voice, to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without Low Latency Queueing, CBWFQ provides weighted fair queueing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion.

For CBWFQ, the weight for a packet belonging to a specific class is derived from the bandwidth you assigned to the class when you configured it. Therefore, the bandwidth assigned to the packets of a class determines the order in which packets are sent. All packets are serviced fairly based on weight; no class of packets may be granted strict priority. This scheme poses problems for voice traffic, which is largely intolerant of delay, especially variation in delay. For voice traffic, variations in delay introduce irregularities of transmission manifesting as jitter in the heard conversation.

The Low Latency Queueing feature provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Configured by the **priority** command, Low Latency Queueing enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue.

In the event of congestion, when the bandwidth is exceeded, policing is used to drop packets. Voice traffic enqueued to the priority queue is User Datagram Protocol (UDP)-based and therefore not adaptive to the early packet drop characteristic of Weighted Random Early Detection (WRED).

When congestion occurs, traffic destined for the priority queue is metered to ensure that the bandwidth allocation configured for the class to which the traffic belongs is not exceeded. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120xe/120xe5c/llqvip.htm

New Revision of System Controller Chip for NPE-175/NPE-225

Platforms: Cisco 7200 series

This feature adds support for a new revision of a hardware component that fixes a previous error. For the benefit of users that have not upgraded to the new hardware, it will also exhibit the following warning error message that indicates the old hardware revision:

```
PLATFORM-4-RECALLED_NPE: Old version NPE-175/225 with Rev= 0xNN system controller.
Contact upgrades-info@cisco.com for replacement.
```

Cisco 7200 series routers with NPE-175 or NPE-225 network processing engines must upgrade to Cisco IOS releases that incorporate this change (for example, Cisco IOS Release 12.0(9) and later releases or Cisco IOS Release 12.0(9)S and later releases). Use of older Cisco IOS releases might result in unpredicted malfunctions. See the following document for further information:

http://www.cisco.com/warp/customer/770/fn8611.shtml

Route Switch Processor (RSP8)

Platforms: Cisco 7500/RSP series

The RSP8 is the newest main system processor module for Cisco 7500 series routers. In addition to running the system software from DRAM, the RSP8 sends and receives routing protocol updates, manages tables and caches, monitors interface and environmental status, and provides Simple Network Management Protocol (SNMP) management and the interface between the console and Telnet.

The high-speed switching section of the RSP8 communicates with and controls the interface processors on the high-speed CyBus. This switching section of the RSP8 decides the destination of a packet and switches it based on that decision. See the following document for further information:

www.cisco.com/cc/td/doc/product/core/cis7507/7507cfig/6586rsp8.htm

Router-ports Group Management Protocol (RGMP)

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Router-Port Group Management (RGMP) is a new protocol that restricts multicast traffic to router ports.

CGMP (Cisco Group Management Protocol) and IGMP (Internet Group Management Protocol) are two existing features that restrict multicast traffic to hosts that do not need to receive them, reducing the amount of processing the hosts have to do. CGMP and IGMP only restrict traffic on the ports of switches to which hosts are connected. CGMP and IGMP are designed for typical access networks where many hosts are connected but only one or two routers forward traffic to those hosts.

RGMP is designed for switched backbone networks or exchange points where predominantly routers are connected to each other. Large amounts of multicast traffic can be restricted, eliminating unnecessary congestion on the router ports. To effectively restrict multicast traffic to router ports, both the routers and the switches on the network must support RGMP.

New Features in Cisco IOS Release 12.0(8)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced in other Cisco IOS releases. For more complete information, refer to the original release.

APS Reflector Mode

Platforms: Cisco 12000 series

APS reflector mode enhances the operation of automatic protection switching (APS) by decreasing the remote timeout that occurs when a remote router is informed of a switchover between the working router and protect router in an APS circuit.

Cisco 12016 Gigabit Switch Router

Platforms: Cisco 12000 series

The Cisco 12016 Gigabit Switch Router (GSR), is a 16-slot member of the Cisco 12000 series of Gigabit Switch Routers. The Cisco 12016 GSR delivers a raw transmission rate per slot of up to 10 Gbps, a switching capacity of up to 160 Gbps, and speeds of up to OC-48/STM-16 (2.44 Gbps). It uses the same Gigabit Route Processor (GRP) and line cards (OC-3, OC-12, and OC-48) as the other routers in the Cisco 12000 series of routers. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12016/hfricg/index.htm

Enhanced Quad OC-12c/STM-4c Layer 3 Packet-over-SONET Line Card

Platforms: Cisco 12000 series

The Quad OC-12c/STM-4c Packet-over-SONET (POS) line card provides Cisco 12000 series routers with four 622-Mbps POS interfaces on a single card. The card interfaces with the switch fabric in the Cisco 12000 series router and provides four OC-12c/STM-4c duplex SONET connections via Single-Mode OC-3c Cable (SC Connectors). Each connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/10187pos.htm

Fast EtherChannel Support on Cisco 7200 Platform

Platforms: Cisco 7200 series

Fast EtherChannel is now supported on Cisco 7200 series routers. The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. For more information on Fast EtherChannel, see the original feature guide written for the 11.1 CC Release, *Fast EtherChannel*, at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/ca111/fechan.htm

Or see page 31 of the *Cisco IOS Interface Configuration Guide* for Cisco IOS Release 12.0 at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/inter_c/iclanint.htm#3809

Multiprotocol Label Switching Traffic Engineering OSPF Support

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Multiprotocol Label Switching (MPLS) traffic engineering software released in Cisco IOS Release 12.0(5)S has been enhanced to support OSPF routing. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s8/te_1208s.htm

Service Assurance Agent

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key service level agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

The SA Agent feature was introduced in Cisco IOS Release 12.0(5)T, and is now available in Cisco IOS Release 12.0(8)S.

The SA Agent provides new capabilities that enable you to monitor:

- Domain Name System (DNS) performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP) echo response time, and TCP connection setup time, with different ToS settings in the IP header.
- Network one-way delay variance (jitter) and packet loss.
- Web server response time.

See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/saaoper.htm

Virtual Path Traffic Shaping

Platforms: Cisco 12000 series

Virtual path (VP) traffic shaping allows multiple virtual circuits (VCs) to be bundled into one VP. This "bundling" is also called traffic shaping because all VCs bundled within the VP are shaped as one traffic rate. In addition, bundling the VCs improves the error detection for the bundled VCs.

New Features in Cisco IOS Release 12.0(7)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced in other Cisco IOS releases. For more complete information, refer to the original release.

ATM CLP Setting

Platforms: Cisco 7500/RSP series

The use of the Cell Loss Priority (CLP) bit in the ATM header of a cell provided a method of controlling the discarding of cells in a congested ATM environment. A CLP bit contains two settings: 0 or 1. Cells with a CLP bit setting of 1 are discarded before cells with a CLP bit setting of 0. Before the introduction of the ATM CLP Setting feature, the CLP bit was automatically set to 0 when Cisco routers converted packets into ATM cells for ATM networks.

The ATM CLP Setting feature allows users to control the CLP bit setting on routers running the PA-A3 port adapter. CLP bits are set on each packet individually, and the default CLP bit setting is 0. The application of the ATM CLP feature changes the CLP bit setting to 1. Therefore, users have the option of leaving each packet with the default CLP bit setting of 0 or establishing a new CLP bit setting of 1. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s7/atmclp.htm

Distributed Traffic Shaping

Platforms: Cisco 7500/RSP series

Many enterprise and service provider customers need to shape traffic in their networks and sometimes need to shape IP traffic independently of the underlying interface. In other cases, the goal is to perform traffic shaping to ensure adherence to committed information rates on Frame Relay links.

The dTS feature is one element used to manage the bandwidth of an interface to avoid congestion, meet remote site requirements, and conform to a service rate that is provided on that interface.

The distributed Traffic Shaping (dTS) feature uses queues to buffer traffic surges that can congest a network. Data is buffered and then sent into the network at a regulated rate, which ensures that traffic will behave in accordance with the configured descriptor, as defined by committed information rate (CIR) (mean rate), Bc (burst size), and Be (excess burst size). With the defined average bit rate and burst size that are acceptable on that shaped entity, you can derive a time interval value.

The excess burst size (Be) allows more than the burst size to be sent during a time interval under certain conditions. Therefore, dTS provides two types of **shape** commands: **average** and **peak**. When **shape average** is configured, the interface sends no more than the burst size for each interval, achieving an average rate no higher than the mean rate (CIR). When **shape peak** is configured, the interface sends Bc plus Be bits in each interval.

In a link layer network such as Frame Relay, the network sends messages with the forward explicit congestion notification (FECN) or backward explicit congestion notification (BECN) if there is congestion. With the dTS feature, the traffic shaping adaptive mode takes advantage of these signals and adjusts the traffic descriptors, which approximates the rate to the available bandwidth along the path.

Enhanced OC-48c/STM-16c Layer 3 Packet-over-SONET Line Card

Platforms: Cisco 12000 series

The OC-48c/STM-16c POS line card provides Cisco 12000 series routers with a single 2.5-Gbps POS interface on a single card. The card interfaces with the switch fabric in the Cisco 12000 series router and provides one OC-48c/STM-16c duplex SC or FC single-mode connection. This connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/6792oc48.htm

Gigabit Ethernet (PA-GE Support)

Platforms: Cisco 7200 series

The PA-GE is a single-port port adapter that, when combined with the appropriate fiber-optic cable and a Gigabit Interface Converter (GBIC), provides one Gigabit Ethernet (GE) interface that is compliant with the IEEE 802.3z specification. The GE interface on a PA-GE operates in full-duplex mode. The PA-GE is supported by the Cisco 7200 VXR routers. Please note that this port adapter is not currently supported by the fourth-generation Versatile Interface Processor (VIP4). See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/72vxpa/7188page/index.htm

ISIS Over ISL

Platforms: Cisco 7200 series, Cisco 7500/RSP series

With release 12.0(7)S, Intermediate System-to-Intermediate System (ISIS), Connectionless Network Service (CLNS), and Interior Gateway Routing Protocol (IGRP) configuration commands are now recognized on an Inter-Switch Link (ISL) virtual LAN (VLAN) subinterface.

MPLS Switching Support for Gigabit Ethernet

Platforms: Cisco 12000 series

Basic tag/Multiprotocol Label Switching (MPLS) switching is now supported for Gigabit Ethernet (GE) line cards for the Cisco 12000 series Gigabit Switch Router (GSR).

NetFlow Support for Gigabit Ethernet

Platforms: Cisco 12000 series

The NetFlow feature is now a supported feature for Gigabit Ethernet (GE) line cards for the Cisco 12000 series Gigabit Switch Router (GSR).

Per-VC Queueing

Platforms: Cisco 12000 series

The per-virtual circuit (VC) queueing enhancements for the Quad OC-3c/STM-1c ATM line card provide additional control of traffic management on the line card. Within limits, you can adjust queuing priorities for each VC defined on a line card interface. This feature lessens traffic congestion and improves quality of service (QoS).

Two-Port Multichannel DS1/PRI and Multichannel E1/PRI Port Adapters

Platforms: Cisco 12000 series

Two-port versions of the Multichannel DS1/PRI and Multichannel E1/PRI port adapters are now available. See the following documents for further information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/4815ds1p/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/5083e1p/index.htm

New Features in Cisco IOS Release 12.0(6)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced in other Cisco IOS releases. For more complete information, refer to the original release.

1OC-12/STM-4 SRP Line Card

Platforms: Cisco 12000 series

The 1OC-12/STM-4 spatial reuse protocol (SRP) line card equips the Cisco series 12000 Gigabit Switch Router with a total of two OC-12c, fiber-optic SC duplex ports. The line card provides two duplex SC connections for either the single-mode or multimode version. The Service Processing Element (SPE) payload is concatenated, which increases efficiency by eliminating the need to partition the bandwidth. The 1OC-12/STM-4 SRP line card is slot independent. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/5929srp.htm

6DS3-SMB Line Card

Platforms: Cisco 12000 series

The 6DS3-SMB line card consist of high-density DS3 service through six T3 interfaces.

The 6-port line card is a partially depopulated version of the 12-port line card. The 6-port line card consists of a total of 12 connectors. A single port consists of one coaxial connector for receiving (Rx) and one coaxial connector for sending (Tx). The ports on the 6-port line card are numbered 0 to 5.

The 6DS3-SMB line card supports serial encapsulation protocols, Gigabit Switch Router (GSR) standard line card packet switching, and DS3 support. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/6587ds3.htm

8-Port Fast Ethernet Line Card

Platforms: Cisco 12000 series

The 8-Port Fast Ethernet line card provides eight Fast Ethernet (IEEE 802.3u) interfaces that operate at a full-duplex data rate of 100 Mbps each. This line card connects to the Gigabit Switch Router (GSR) switch fabric, which supports transfer rates of up to 40 Gbps within the GSR.

The 8-Port Fast Ethernet line card supports both copper and fiber-optic Fast Ethernet transceivers. The fiber-optic 100BaseFX interface supports multimode SC duplex connectors operating in half- or full-duplex mode. The copper interface supports both full- and half-duplex 100BaseTX standards that use an RJ-45 connector.

The Fast Ethernet connectivity gives the GSR platform the flexibility to be used as an edge router in high-bandwidth environments, such as an Internet service provider or a corporate backbone. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis12012/bfrcfig/6224fe8.htm

Memory Scan

Platforms: Cisco 7500/RSP series

The Memory Scan feature for Cisco 7500 series router Route Switch Processor (RSP) modules adds a low-priority background process that searches all installed DRAM for possible parity errors. The process runs every 60 seconds and can be controlled and monitored with new command-line interface commands. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/tmemscn.htm

NetFlow Policy Routing

Platforms: Cisco 7500/RSP series

IP policy routing now works with Cisco Express Forwarding (CEF), distributed CEF (dCEF), NetFlow, and NetFlow with flow acceleration.

IP policy routing was formerly supported only in fast switching and process-switching. Furthermore, support in fast switching was limited because the routing table sometimes had to be consulted before packets could be policy-routed, which was too expensive or impossible in the fast-switching path.

NetFlow on GSR

Platforms: Cisco 12000 series

NetFlow routing is now supported on the Cisco 12000 series routers. Support for Netflow routing on the Gigabit Ethernet port adapter, PA-GE, is not yet available.

NPE-175/NPE-225

Platforms: Cisco 7200 series

The network processing engine is available in five versions: NPE-150, NPE-175, NPE-200, NPE-225, and NPE-300. The network processing engines have the same functionality; however, the performance differs because of the microprocessor type and the type of memory for packet data (SRAM and DRAM, or SDRAM) each network processing engine provides.

The latest network processing engines, the NPE-175 and NPE-225, consist of two modular boards: the processing engine and the network controller board. SRAM is not included in the NPE-175 or NPE-225.

OC-12c Dynamic Packet Transport Port Adapter

Platforms: Cisco 7200 series, Cisco 7500 series

The Dynamic Packet Transport (DPT) port adapter is a dual-width OC-12c port adapter that provides a shared IP over SONET capability in a Cisco 7200 series, Cisco 7200 VXR, or Cisco uBR7200 series router.

The DPT port adapter is designed to be deployed in SONET OC-12 DPT rings. DPT rings can also be connected to SONET add drop multiplexers (ADMs), thus allowing for the creation of small or very large DPT rings. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206cfig/6481oc12.htm

PA-MC-2T3+ Multichannel T3 Port Adapter

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-MC-2T3+ is a single-width port adapter that provides two T3 interface connections using BNC connectors. The interface can provide up to 28 T1 lines (a single T3 group). Each T1 line is presented to the system as a serial interface that can be configured as one or more serial interfaces.

The PA-MC-2T3+ is a channelized port adapter that sends and receives data bidirectionally at the T3 rate of 44.736 Mbps (digital signal carried on a T3 line, DS3). The T3 connection, provided by two female BNC connections for transmit (TX) and receive (RX), requires 734A coaxial cable that has an impedance of 75 ohms.

On the VIP2, PA-MC-2T3+ microcode is loaded into and operates from synchronous dynamic random-access memory (SDRAM) on the VIP2-50. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206cfig/64452t3/index.htm

Process MIB

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by Sample Network Management Protocol (SNMP). The CISCO-PROCESS-MIB provides CPU 5-second, 1-minute, and 5-minute statistics. In addition, this MIB provides CPU utilization and memory allocation and deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for Versatile Interface Processor (VIP) cards and the master CPU occurs even if the SNMP subsystem is not initialized.

SNMPv3

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large-scale deployment of SNMP for configuration, accounting, and fault management. Currently SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities that make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP strategy. Each SNMP device has an identifier called the SNMP EngineID, which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or an intranet. The SNMPv3 protocol consists of the specification for the User-based Security Model (USM).

Definition of security goals where the goals of message authentication service includes the following protection strategies:

- Modification of information, or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal
- Masquerade, or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- Message stream modification, or protection against messages getting maliciously reordered, delayed, or replayed in order to effect unauthorized management operations
- Disclosure, or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy:
  - Communication without authentication and privacy (NoAuthNoPriv)
  - Communication with authentication and without privacy (AuthNoPriv)
  - Communication with authentication and privacy (AuthPriv)

Turbo Access Control Lists

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The turbo access control lists feature enables Cisco 7200 and 7500 series routers, and Cisco 12000 series Gigabit Switch Routers (GSRs) to evaluate access control lists (ACLs) for more expedient packet classification and access checks.

New Features in Cisco IOS Release 12.0(5)S

Many of the new features in Cisco IOS Release 12.0 S were originally introduced in other Cisco IOS releases. For more complete information, refer to the original release.

ATM PVC Trap Support

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The ATM PVC Trap Support feature provides Simple Network Management Protocol (SNMP) notification for permanent virtual circuit (PVC) failures, and it provides SNMP access to PVC status tables.

Normally, a management station is not notified when an ATM PVC goes down. The ATM PVC Trap Support feature enables an agent to send the required PVC traps for this notification. It also provides support for these PVC status tables: atmCurrentlyFailingPVclTable and atmInterfaceExtTable.

Available Bit Rate Servicing and Virtual Path Shaping on PA-A3 Port Adapters

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-A3 ATM port adapters (PA-A3-T3, PA-A3-E3, PA-A3-OC3MM, PA-A3-OC3SMI, and PA-A3-OC3SML) available on Cisco 7500 series routers now support the following new features:

- Available bit rate (ABR)—The ABR service category is specified in the ATM Forum Traffic Management Specification Version 4.0.
- Virtual Path Shaping—A virtual path (VP) is a logical association or bundle of virtual circuits (VCs).

The PA-A3 ATM port adapters support multiplexing of one or more VCs over a VP that is shaped at a constant bandwidth. To use this feature, you configure a permanent virtual path (PVP) with a specific virtual path identifier (VPI). Any VCs that are created subsequently with the same VPI are multiplexed onto this VP; the traffic parameters of individual VCs are ignored.

Cisco 7576 Router

Platforms: Cisco 7500/RSP series

The Cisco 7576 router is the newest member of the Cisco 7500 series of routers, which consists of the 5-slot Cisco 7505, 7-slot Cisco 7507, and the 13-slot Cisco 7513. The Cisco 7576 router supports multiprotocol and multimedia routing and bridging with a wide variety of protocols and any combination of available electrical interfaces and media.

The Cisco 7576 router consists of two independent routers configured on a single backplane. This system is housed within the chassis footprint of a Cisco 7513 router. The dual independent router design effectively doubles the system bandwidth that exists in the Cisco 7513 router.

Network interfaces reside on interface processors that provide a direct connection between the two independent dual CyBuses located on the backplane of the Cisco 7576 router and your external networks. The two independent dual CyBuses facilitate the configuration of two independent routers on a single backplane.

There are bays for up to two AC-input or DC-input power supplies. The Cisco 7576 router will operate with one power supply. Although a second power supply is not required, a second power supply allows load sharing and increased system availability. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7576/index.htm

Command Line Interface String Search

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The command line interface (CLI) string search feature allows you to search or filter the output of any **show** or **more** command, which is useful for sorting through large amounts of output, or if you want to exclude output that you do not need to see. CLI string search also allows for searching and filtering at --More-- paging prompts.

With the search function, you can begin unfiltered output at the first line that contains a regular expression you specify. You can specify a maximum of one filter per command to either include or exclude output lines that contain the specified regular expression.

A regular expression is any word, phrase, number, and the like that appears in **show** or **more** command output.

Frame Relay Enhancements for K2 Scalability

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The **logging event** command has been enhanced to enable or disable logging data-link connection identifier (DLCI) Change and subinterface UPDOWN console messages on Cisco 7200 and Cisco 7500 series routers. The **logging event dlci-status-change** and **logging event subif-link-status** commands are used to enable logging.

The display on the **show frame-relay pvc** command has been enhanced on Cisco 7200 and Cisco 7500 series routers to include a table showing the number of permanent virutal connections (PVCs) in their various states.

Gigabit Ethernet Interface Processor

Platforms: Cisco 7500/RSP series

The Gigabit Ethernet Interface Processor (GEIP) is a single-port fixed configuration interface processor that, when combined with the appropriate fiber optic cable, provides one 1000-Mbps Gigabit Ethernet interface that complies with IEEE 802.032 standards.

The Gigabit Ethernet interface operates in full-duplex mode at 1000 Mbps in each direction: transmit (TX) and receive (RX).

The GEIP is available on all Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

An increased maximum Ethernet packet size of 1500 takes advantage of increased bandwidth and the full-duplex point-to-point link.

An interface command MTU (maximum transmission unit) allows users to specify an MTU size up to 16K (maximum supported by FX1000). The minimum allowable MTU size is 1500 bytes.

If the interface is configured with a fall-back option, the other port will be reconfigured to support a large packet when a switchover occurs. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/cis7000/7000cfig/5350geip.htm

Gigabit Ethernet Line Card

Platforms: Cisco 12000 series

The Gigabit Ethernet line card provides Cisco 12000 series routers with an optical Ethernet interface on a single card that operates faster than 1 Gbps. The card interfaces with the switch fabric in the Cisco 12000 series router and provides one Gigabit Ethernet SC single-mode or multimode connection. This connection is concatenated, which provides for increased efficiency by eliminating the need to partition the bandwidth. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/gigecr.htm

GRP Redundant Processor Support

Platforms: Cisco 12000 series

The Gigabit Route Processor (GRP) redundant processor feature allows for the installation of two GRPs in a Cisco 12000 series Gigabit Switch Router. One GRP functions as the primary processor. The primary GRP supports all normal GRP operation. The other GRP functions as the secondary processor. The secondary GRP monitors the primary and will take over normal GRP operations if it detects a failure in the primary GRP. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/gsr_rp.htm

ISL Support

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Inter-Switch Link (ISL) support maintains virtual LAN (VLAN) information as traffic flows between switches and routers. ISL support has been added to the following images for the Cisco 7000 family in Release 12.0(5)S: c7200-p-mz, c7200-k3p-mz, c7200-k4p-mz, rsp-pv-mz, rsp-k3pv-mz and rsp-k4pv-mz.

Multicast BGP

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Multicast Border Gateway Protocol (MBGP) feature adds capabilities to BGP to enable multicast routing policy throughout the Internet and to connect multicast topologies within and between BGP autonomous systems. That is, MBGP is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) to build data distribution trees.

It is possible to configure BGP peers that exchange both unicast and multicast network-layer reachability information (NLRI).

MBGP is useful when you want a link dedicated to multicast traffic, perhaps to limit which resources are used for which traffic. Perhaps you want all multicast traffic exchanged at one network access point (NAP). MBGP allows you to have a unicast routing topology different from a multicast routing topology. Thus, you have more control over your network and resources.

Prior to MBGP, the only way to perform interdomain multicast routing was to use the BGP infrastructure that was in place for unicast routing. If those routers were not multicast capable, or you had differing policies where you wanted multicast traffic to flow, you could not support it. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/mbgp.htm

Multicast Distributed Switching

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Prior to multicast distributed switching (MDS), IP multicast traffic was always switched at the Route Processor (RP) in the Route Switch Processor (RSP)-based platforms. With Cisco IOS Release 11.2 GS and Release 11.1 CC, IP multicast traffic can be distributed switched on RSP-based platforms with Versatile Interface Processors (VIPs).

Furthermore, MDS is the only multicast switching method on the Cisco 12000 Gigabit Switch Router (GSR), starting with Cisco IOS Release 11.2(11)GS.

Switching multicast traffic at the RP has the following disadvantages:

- The load on the RP is increased. This increase affects important route updates and calculations (for BGP, among others) and can stall the router if the multicast load is significant.
- The net multicast performance is limited to what a single RP can switch.

MDS solves these problems by performing distributed switching of multicast packets received at the line cards (VIPs in the case of an RSP, and line cards in the case of a GSR). The line card is the interface card that houses the VIPs (in the case of RSP) and the GSR line card (in the case of a GSR). MDS is accomplished using a forwarding data structure called a Multicast Forwarding Information Base (MFIB), which is a subset of the routing table. A copy of MFIB runs on each line card and is always kept up to date with the RP MFIB table.

In the case of RSP, packets received on non-VIP interface processors are switched by the RP.

MDS can work in conjunction with Cisco Express Forwarding (CEF), unicast distributed fast switching (DFS), or flow switching. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/mds.htm

Multicast Routing Monitor

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

The Multicast Routing Monitor (MRM) feature is a management diagnostic tool that provides network fault detection and isolation in a large multicast routing infrastructure. It is designed to notify a network administrator of multicast routing problems in near real time.

MRM has three components that play different roles: the Manager, the Test Sender, and the Test Receiver. The Manager can reside on the same device as the Test Sender or Test Receiver. You can test a multicast environment using test packets (perhaps before an upcoming multicast event), or you can monitor existing IP multicast traffic.

You create a test based on various test parameters, name the test, and start the test. The test runs in the background and the command prompt returns. If the Test Receiver detects an error (such as packet loss or duplicate packets), it sends an error report to the router configured as the Manager. The Manager immediately displays the error report. Also, by issuing a certain **show** command, you can see the error

reports, if any. You then troubleshoot your multicast environment as normal, perhaps using the **mtrace** command from the source to the Test Receiver. If the **show** command displays no error reports, the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

Multicast Source Discovery Protocol

Platforms: Cisco 7200 series, Cisco 7500/RSP, Cisco 12000 series

Multicast Source Discovery Protocol (MSDP) connects multiple Protocol Independent Multicast (PIM) sparse-mode (SM) domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection, where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal, source-tree building mechanism in PIM-SM.

MSDP is also used to announce sources sending to a group. These announcements must originate at the domain RP.

MSDP depends heavily on MBGP for interdomain operation. You should run MSDP in your domain RPs that act as sources, sending to global groups for announcement to the Internet. See the following document for futher information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t7/msdp.htm

Multiprotocol Label Switching Traffic Engineering

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. Traffic engineering is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures.

MPLS traffic engineering provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

MPLS traffic engineering routes traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.

MPLS traffic engineering employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow. In MPLS traffic engineering, the flow has bandwidth requirements, media requirements, a priority versus other flows, and so on.

MPLS traffic engineering gracefully recovers to link or node failures that change the topology of the backbone by adapting to the new set of constraints. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s5/mpls_te.htm

NPE-300

Platforms: Cisco 7200 series

The network processing engine NPE-300 is the newest and the highest performance processor in the family of network processing engines for the Cisco 7200 series routers. The NPE-300 performs at a rate of approximately 300,000 packets per second (pps) in fast switching, a 50 percent increase over the NPE-200 performance.

The NPE-300 uses a high-performance 262.5-MHz R7000 RISC processor and can support up to 256 MB of memory, providing superior performance for both enterprise and service provider applications that require processor-intensive services. Network layer services such as traffic management, security, and QoS benefit significantly from the high performance of NPE-300.

A Cisco 7200 VXR router equipped with an NPE-300 can support up to six high-speed port adapters and can also support higher-speed port adapter interfaces including Gigabit Ethernet and OC-12 ATM. The NPE-300 uses synchronous DRAM (SDRAM) for storing all packets received or sent from network interfaces. The SDRAM also stores routing tables and network accounting applications. There are two independent SDRAM memory arrays in the system that allow concurrent access by port adapters and the processor. The NPE-300 can be configured with up to 256 MB of processor and packet memory, which is double the 128-MB memory limit on the NPE-200. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/core/7200vx/72vxicg/index.htm

PA-MC-8EI/120, PA-MC-4TI, PA-MC-8TI, and PA-MC-8DSX1 Multichannel E1 and T1 ISDN PRI Port Adapters

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The multichannel E1 and T1 ISDN PRI port adapters (PA-MC-8E1/120, PA-MC-4T1, PA-MC-8T1, and PA-MC-8DSX1) are available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

The PA-MC-8E1/120, PA-MC-4T1, and PA-MC-8T1 are single-wide modules that integrate channel service unit (CSU) functionality, data service unit (DSU) functionality, and E1 or T1 channel support into the Cisco router. The PA-MC-8DSX1 is a single-wide module that integrates DS1 DSU functionality and DS0 channel support into the Cisco router.

The PA-MC-8E1/120, PA-MC-4T1, PA-MC-8T1, and PA-MC-8DSX1 provide four or eight independent T1 (100-ohm) or E1(120-ohm) connections via RJ-48C connectors. Each T1 or E1 port adapter can provide up to 128 separate full-duplex High-Level Data Link Control (HDLC) fractional or full T1 or E1 channels. Individual T1 connections of the DSX-1 version of the port adapters can connect to external CSUs, to digital cross connects (DACS), or to any other equipment that uses a DSX-1 interface.

See the following documents for further information:

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/4815ds1p/index.htm

http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cfig_nts/5083e1p/index.htm

PA-MC-E3 Multichannel E3 Synchronous Serial Port Adapter

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-MC-E3 Multichannel E3 synchronous serial port adapter is available on Cisco 7200 series routers, Cisco 7500 series routers, and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). The PA-MC-E3 has one channelized E3 high-speed serial interface that provides access to services at E1 (2.048 Mbps) data rates, transferring data bidirectionally. This port adapter divides the E3 signal stream into 16 E1 lines that can be further divided to the 64-kbps level, up to a total of 128 channels. The PA-MC-E3 complies with Consultative Committee for International Telegraph and Telephone/International Telecommunication Union (CCITT/ITU) G.703 physical layer standards and CCITT/ITU G.751 for E3, G.742 for E2, and G.704 and G.706 for E1 fault and alarm detection and response actions. The E1 lines can be configured as channelized, fractional, and unframed. PRI ISDN will be supported in a later release. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/pamce3.htm

PA-MC-T3 Multichannel T3 Port Adapter

Platforms: Cisco 7200 series, Cisco 7500/RSP series

The PA-MC-T3 Multichannel T3 port adapter is available on Cisco 7200 series routers, second-generation Versatile Interface Processor (VIP2) in Cisco 7500 series routers, and the Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI).

The PA-MC-T3 has one channelized T3 high-speed serial interface that provides access to services at T1 data rates, transferring data bidirectionally.

This port adapter divides the T3 signal stream into 28 T1 lines that can be further divided into the 64 kbps level, up to a total of 128 channels. See the following document for further information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/pamct3.htm

RFC 1483 Bridged PVC Encapsulation

Platforms: Cisco 12000 series

Using RFC 1483 bridged permanent virtual connection (PVC) encapsulation on a Cisco 12000 series router, a Gigabit Switch Router (GSR) ATM interface can be connected directly to a Catalyst 5000 series switch ATM port. When configuring the GSR ATM interface, you must create a new 1483 half-bridge PVC connection using a multipoint subinterface. Only one PVC half-bridge connection per subinterface is allowed; however, other non-PVC connections (SVC or nonbridged PVC) are allowed on the subinterface. Configure an MTU size of 1500 so that the Catalyst switch will not drop packets. Full bridging in the GSR is not supported. Also note that Ethernet format is supported. IEEE 802.3 format is not supported at this time.

Secure Shell Version 1

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a router. Two versions of SSH are available, SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in Cisco IOS software.

The SSH server feature enables an SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to an inbound Telnet connection. The SSH server in Cisco IOS will work with publicly and commercially available SSH clients.

Before SSH, security was limited to Telnet security. SSH allows strong encryption to be used with Cisco IOS authentication.

Tag Switching

Platforms: Cisco 7200 series, Cisco 7500/RSP series, Cisco 12000 series

Tag switching is a novel approach to network layer packet forwarding. The two main components of the tag switching architecture are forwarding and control. Forwarding is accomplished using simple label-swapping techniques, while the existing network layer routing protocols plus mechanisms for binding and distributing tags are used for control. Tag switching can retain the scaling properties of IP and can help improve the scalability of IP networks.

Important Notes

Important Notes for Cisco IOS Release 12.0(13)S

Cisco 7500/RSP Series Images Deferred

Four images were deferred in Cisco IOS Release 12.0(13)S due to severe defects. The following images are affected:

- rsp-boot-mz
- rsp-pv-mz
- rsp-k3pv-mz
- rsp-k4pv-mz

The following defects caused the deferral of these images:

- CSCds58988—Nested r4k_return_to_monitor calls, 75xx will not boot (HSA)
- CSCds49677—3xGE - GRP-3-ENCAP:Failure to allocate, slot X (info 0x22)
- CSCds17084—MQC:change q-limit then remove the policy would cause RSP crash
- CSCds50637—changes in GSR ACL config may reduce performance
- CSCds30549—sh ip bgp summ shows incorrect number of received prefixes
- CSCds61573—ATMOC3-LC stops packet forwarding from 3PortGigE w/egress CAR cnfg
- CSCdr47814—ifTable ATM0/0.0 subinterface shows up w/o any pvcs configured
- CSCds62557—VIP4-50 performance

- CSCdr76940—MPLS loadsharing inconsistincy for 0.0.0.0
- CSCds56717—sh tag for shows untagged while remote binding is available
- CSCds58727—cannot ping across mpls te tunnel
- CSCdr42215—SRP needs to run service downl - fl to upgrade rom vers permanentl
- CSCdp24155—ISIS:(route-leaking) local L2 interfaces not redistributed into L1

This release has been replaced with the following software solution(s), which are available on CCO:

- 12.0(13)S2

In order to increase network availability, Cisco recommends that you upgrade affected IOS images with the suggested replacement software images. Cisco will discontinue manufacturing shipment of affected IOS images. Any pending order will be substituted by the replacement software images.

Caution Please be aware that failure to upgrade the affected Cisco IOS images may result in network downtime.

The terms and conditions that governed your rights and obligations and those of Cisco, with respect to the deferred images will apply to the replacement images.

Important Notes for Cisco IOS Release 12.0(10)S

Unicast RPF—New ACL Bypass and Logging Functions

Access Control List (ACL) functions have been added to the Unicast RPF feature that will allow new logging capability and exceptions to Unicast RPF checks. Interface-specific counters for Unicast RPF drops have been included in **show ip interface**.

The **ip verify unicast reverse-path** [*acl*] command enables the checking of source IP addresses in packets that are being Cisco Express Forwarding (CEF) or distributed Cisco Express Forwarding (dCEF)-switched. If the source IP address is known to be reachable through the interface from which the packet was received, the packet is forwarded. Otherwise, the packet is dropped and counted once on the interface over which the packet was received and once globally. The interface counter is part of the **show ip int** *int* output, and the global counter is part of the **show ip traffic** output.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

This section contains only open caveats for the current Cisco IOS 12.0 S maintenance release.

Because Cisco IOS Release 12.0 S is based on Cisco IOS Release 12.0, many caveats that apply to Cisco IOS Release 12.0 will apply to Cisco IOS Release 12.0 S. For information on severity 1 and 2 caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0* located on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at http://www.cisco.com/support/bugtools.

Open Caveats—Cisco IOS Release 12.0(14)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(14)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdm71776

  If the **slave auto-sync config** global configuration command is enabled on a High System Availability (HSA) system and you enter the **config-register** global configuration command followed by the **write memory** command, the master system configuration register will be set to change on the next reboot, but the slave configuration register will not be set to change.

  Workaround: Enter the **slave sync config** privileged EXEC command, which will update the slave configuration register for the next reboot.

- CSCdp19943

  The online insertion and removal (OIR) of a slave Route Switch Processor (RSP) might cause the master to exhibit RSP-3-BAD BUFHDR messages. There is no workaround.

- CSCdr06282

  A Cisco RSP8 Route Switch Processor (RSP) might run out of buffer headers used for communication between the Versatile Interface Processors (VIPs) and the RSP. This situation usually occurs on a Cisco 7500 series router that is configured with several T1 port adapters (PAs). Communication between the VIP and the RSP is adversely affected, and messages, such as the VIP notifying the RSP that a line has gone down, might not be completed. You can diagnose this condition by using the **show controllers cbus** privileged EXEC command to determine if the number of buffers in BufhdrQ is near zero. There is no workaround.

- CSCdr13342

  A Versatile Interface Processor (VIP) that is running distributed Cisco Express Forwarding (dCEF) might exhibit the following error message:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 5: No window message, LC to RP IPC is
  non-operational
  ```

  After this error message has been displayed, packets that are traveling on the interfaces of the VIP might be misdirected. This situation can be fixed by entering the **clear cef linecard** [*slot-number*] EXEC command, but the VIP might reload with a memory corruption shortly after the command is entered if the VIP is under a very high load. There is no workaround.

- CSCdr35103

  The SA-COMP compression service adapter (CSA) is supported only on VIP2-50 Versatile Interface Processors (VIPs) with revision C0 or later revisions. If the SA-COMP CSA is used with an earlier revision, the router will experience a VIP reload, and the VIP will become disabled. There is no workaround.

- CSCdr52041

  A Cisco 7500/RSP series router with an RSP4 Route Switch Processor that is running the rsp-pv-mz.120-10.S.bin image might exhibit QA errors, and the RSP might restart with a cBus complex. In at least one instance, this condition occurred after the router was upgraded from Cisco IOS Release 12.0(9)S because of Multiprotocol Label Switching (MPLS) problems. There is no workaround.

- CSCdr66353

  A Cisco router with a Network Processing Engine-300 (NPE-300) that is running Cisco IOS Release 12.0(10)S might reload when the temperature on outlet 3 of the NPE reaches a warning temperature. When the temperature in outlet 3 has reached a warning state for a high temperature, the following error message is exhibited:

  ```
  %ENVM-4-ENVWARN: chassis outlet 3 measured at 52C/125F
  ```

  There is no workaround.

- CSCdr71075

  The following problems have been observed in Cisco IOS Release 12.0(10.3)S:

  – The ifNumber that is returned by Simple Network Management Protocol (SNMP) is incorrect.

  – Frame Relay subinterfaces are missing from the ifTable and the ifXTable.

  – The ifStackTable does not exhibit the same number of interfaces as is indicated by ifNumber ifIndices.

  There is no workaround.

- CSCdr78008

  A Cisco 7200 series router with hardware compression enabled on BRI interfaces might pause indefinitely, and console access will be lost.

  Workaround: Disable the hardware compression on the affected interfaces, or use software compression.

- CSCds25165

  A Cisco Route Switch Processor 8 (RSP8) might enter into an indefinite loop at bootup and display "%SYS-2-INTSCHED:'eventdimiss'" messages at level 6 without dropping to the ROMMON prompt if a **boot host tftp:**[[[*//host*]/*directorypath*]/*filename*] configuration command is present in the startup configuration. See CSCds25135, page 57 for further information.

  Workaround: Change the URL syntax in the configuration command to use the IP address instead of the host name. For example, use **boot host tftp:**[[[*//a.b.c.d*]/*directorypath*]/*filename*].

- CSCds30675

  If a Cisco 7500/RSP series router has the configuration register set so that the router returns to the ROM Monitor after a reload or fatal error occurs (instead of resetting and reloading after a reload or fatal error), you will be unable to access a flash disk or flash card in one of the PCMCIA slots from the ROM Monitor after the router is reset.

  Workaround: Perform a power cycle on the router.

- CSCds52207

  A Cisco 7500/RSP series router might reload with an arithmetic exception at shape_command when traffic shaping is being configured. There is no workaround.

Interfaces and Bridging

- CSCdp81786

  Enabling distributed Cisco Express Forwarding (dCEF) on a Cisco 7500 series router that is running Packet-over-SONET (POS) IP might cause the router to experience repeated Versatile Interface Processor (VIP) reloads.

  Workaround: Disable dCEF.

- CSCds20358

  Under certain circumstances, numerous "ignore" messages might be displayed on a PA-A1 port adapter interface. The output of the **show controllers cbus** command and the **show vip accu** command is clean.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command.

- CSCds21729

  A Versatile Interface Processor (VIP) on a Cisco 7500/RSP series router running Cisco IOS Release 12.0(9)S might reload with a bus error when the processor memory on that VIP is low. The cause of the reload in the crashinfo file is an "ALIGN-1-FATAL" message.

  Temporary workaround: Reduce memory usage on the VIP (for example, by disabling distributed Cisco Express Forwarding (dCEF)).

- CSCds24213

  The channelized interface on a Channelized T3 (CT3) card stops passing traffic. In this situation, the **show controllers cbus** privileged EXEC command shows the txlimit value pegged down to 0:

  ```
  Serial2/1/0/4:1, txq 48001A18, txacc 4800009A (value 0), txlimit 10
  ```

The **show controllers** privileged EXEC command on the Versatile Interface Processor (VIP) card shows the following error messages:

```
Tx bad vc 6
Syslog show : %CBUS-4-FIXBADTXVC: Detected and fixed bad tx vc encap on
Serial2/1/0/26:0, bad vc 0, fixed vc 24
LINK-2-INTVULN: In critical region with interrupt level=0, intfc=Serial1/0:22 -Process=
"ct3sw_periodic 1", ipl= 0, pid= 48
```

Workaround: Type **tx-limit** *5* on the interface and change the queuing mechanism. The change in the queuing mechanism stops the draining and prevents the value from draining to zero again, even if the tx-limit 5 is increased.

- CSCds32322

  A Cisco 7500 series router with a PA-CT3 port adapter that has been channelized down to a T1 might exhibit the following error messages on any of the channelized interfaces when Weighted Fair Queueing is enabled on the interface:

  ```
  %RSP-3-RESTART: cbus complex
  %RSP-3-RESTART: interface Serial5/0/0:1, output stuck
  ```

  In this condition, the channelized interfaces might enter a down/down state, and you will need to reload the router. There is no workaround.

- CSCds40737

  SONET MIBs for Packet-over-SONET (POS) port adapters are not updated on Cisco 7500/RSP series routers. There is no workaround.

- CSCds66853

  A Versatile Interface Processor (VIP) with a Channelized T3 (CT3) port adapter may reload. There is no workaround.

IP Routing Protocols

- CSCdr21205

  Resource Reservation Protocol (RSVP) might tear down a session during a brief carrier state transition on a serial interface even if the line protocol state remains up during the transition. There is no workaround.

- CSCds40571

  A Cisco router that is running Enhanced IGRP (EIGRP) may reload because of a software-forced reload. There is no workaround.

- CSCds41275

  Upgrading to Cisco IOS Release 12.0(12.5)S may cause the OSPF routing process to run with 99 percent CPU utilization and cause low memory problems.

  Possible workaround: Remove and reconfigure the OSPF routing process using the **router ospf** global configuration command.

- CSCds42335

  A Cisco router might reload with a bus error at PC 0x605C7D44, address 0xD0D0D10 that indicates a problem with OSPF. There is no workaround.

- CSCdr63002

  When a Border Gateway Protocol (BGP) inbound route map is configured for a neighbor but the route map is not defined, then the first prefix in the update is rejected. All other prefixes in the update are accepted.

  Workaround: Correct the configuration to remove the configured route map for the neighbor or to create a corresponding route-map.

- CSCds57086

  A Cisco 12000 series Gigabit Switch Router (GSR) might reload with the following error message after the **show ip bgp neighbors** EXEC command is entered:

  ```
  System was restarted by bus error at PC 0x6010E004, address 0xD0D0D0D
  ```

  There is no workaround.

- CSCds59805

  An area border router (ABR) that is generating a default route type 7 for a Not-So-Stubby-Area (NSSA) may max-age the link-state advertisement (LSA) for the default route when you enter the **clear ip ospf redistribution** EXEC command. There is no workaround.

- CSCds64673

  A Cisco router that is running Cisco IOS Release 12.0(10)S may experience alignment errors followed by a software-forced reload after a Border Gateway Protocol (BGP) neighbor flaps. There is no workaround.

Miscellaneous

- CSCdp09791

  If you upgrade a Cisco 7200 series router from Cisco IOS Release 11.1 CC to Cisco IOS Release 12.0(4)S, the Simple Network Management Protocol (SNMP) counters for serial (T1) interfaces might produce unreliable data. The router might experience traffic rates over 10 to 15 Mbps for T1 interfaces.

  All serial T1 interfaces will exhibit this behavior. Serial interfaces on a 4xT1 PA (73-1389-05) and on a Channelized 8xT1 PA (73-2488-05) might also exhibit this behavior. There is no workaround.

- CSCdp20755

  In Cisco IOS Release 12.0 S, fast-switching policy-routed traffic might break when policy-routed fast switching is configured on the tunnel interface itself.

  Workaround: Enter the **tunnel sequence-datagrams** interface configuration command on all tunnel interfaces.

- CSCdp26186

  On a Cisco 12000 series Gigabit Switch Router (GSR), per-subinterface features on Frame Relay subinterfaces are not supported by Channelized OC-12, Packet OC-3 Interface Processor (POSIP), and DS3 line cards. There is no workaround.

- CSCdp39983

  A Cisco Versatile Interface Processor (VIP) 2/40 that is running Cisco IOS Release 12.0(7)S might reload in find_next_non_zero_acl_elem. There is no workaround.

- CSCdp39985

  A Versatile Interface Processor (VIP) 2/40 that is running Cisco IOS Release 12.0(7)S might experience a memory corruption resulting in a software-forced reload. There is no workaround.

- CSCdp58522

  Cisco OC-48c/STM16c and Cisco QOC-12 line cards for the Cisco 12000 series Gigabit Switch Router (GSR) are not differentiating outgoing traffic by protocol type. There is no workaround.

- CSCdp74436

  Entering the **write memory** command simultaneously on both the console and a vty might cause a Cisco router to pause indefinitely. The **write memory** command should not be entered simultaneously on different vtys. There is no workaround.

- CSCdp83097

  A Cisco router that is running Cisco IOS Release 12.0(7)S1 or an earlier release might experience a Versatile Interface Processor (VIP) reload with the following traceback:

  ```
  0x60258C84:tag_fib_iterate(0x60258c08)+0x7c
  0x6025A9BC:tfib_stats_background(0x6025a8e0)+0xdc
  0x6009AFAC:r4k_process_dispatch(0x6009af98)+0x14
  0x6009AF98:r4k_process_dispatch(0x6009af98)+0x0
  ```

  There is no workaround.

- CSCdr03667

  The limitation of VC-per-VP on the Cisco 12000 series Gigabit Switch Router (GSR) is different from the limitation on the Cisco 7500/RSP series router. The Cisco 7500/RSP series router uses software to determine the VC-per-VP value, but the Cisco 12000 series GSR has Segmentation and Reassembly (SAR) hardware that contains a VC-per-VP limitation. This limitation requires the Virtual Channel Identifier (VCI) value to start from 0. There is no workaround.

- CSCdr07940

  A Cisco router might reload if a load-sharing route changes while a **show ip cef detail** command is waiting at the More prompt displaying that route. There is no workaround.

- CSCdr21358

  Cisco Express Forwarding (CEF) per-packet load sharing is not supported when the inbound line card is an Engine 2 (PSA-based) card. This DDTS adds a warning message so that if you attempt to configure per-packet load sharing, the warning message informs you that the feature is not supported. There is no workaround.

- CSCdr35034

  Cisco 12000 series Gigabit Switch Routers (GSRs) do not support non-Multiprotocol Label Switching (MPLS) tunnels, and non-MPLS tunnels should not be configured even though these tunnels are configurable using the command-line interface. There is no workaround.

- CSCdr49770

  A quad OC-3c/STM-1c Packet-over-SONET (POS) line card might reload with a bus error exception when a remote router is disconnected. There is no workaround.

- CSCdr58167

  A Cisco 12000 series Gigabit Switch Router (GSR) might display an “Rx-SAR” error message if the ATM Multi Point-to-Point Switched Virtual Circuit IP Multicast feature is enabled on Engine 0 line cards (for example, a 1-Port OC-12 ATM line card) in a network with approximately 300 Internet Group Management Protocol (IGMP) Multicast groups with 2500 Kbps of Multicast bidirectional traffic.

  Workaround: Reduce the Multicast traffic rate, or do not allow the network to reach 300 IGMP groups.

- CSCdr64558

  If a redundant power supply on a Cisco 12012 Gigabit Switch Router (GSR) is disabled and later reenabled, the GSR might report alarms that relate to fan speed. There is no workaround.

- CSCdr68063

  A Cisco 12000 series Gigabit Switch Router (GSR) may reload if more than 1500 Multiprotocol Label Switching (MPLS) tunnels are configured. There is no workaround.

- CSCdr71218

  A Cisco 12000 series Gigabit Switch Router (GSR) experiences an interprocess communication (IPC) timeout when 400 ATM subinterfaces are configured for tag switching and Intermediate System-to-Intermediate System (IS-IS) and a microcode reload is performed on the ATM line card. A microcode reload should not be performed on the ATM line card in this configuration scheme. There is no workaround.

- CSCdr75832

  A Cisco 12000 series Gigabit Switch Router (GSR) may lose Intermediate System-to-Intermediate System (IS-IS) messages because of a queue overflow if 400 ATM subinterfaces are configured for tag switching and IS-IS. Tag switching should only be enabled on less than 400 subinterfaces. There is no workaround.

- CSCdr77321

  On a Cisco 12000 series Gigabit Switch Router (GSR), an extended access control list (ACL) that denies IP traffic from being sent to a range of IP addresses might deny MPLS-tagged outbound traffic on a 3-port Gigabit Ethernet line card port under the following conditions:

  – MPLS is enabled on the router.

  – An extended ACL is defined that denies IP traffic from being sent to a range of IP addresses (for example, **access-list** *100* **deny** *ip any 3.1.0.0 0.0.255.255*).

  – That extended ACL is applied to inbound traffic on a port of a 3-port Gigabit Ethernet line card (for example, **interface** *GigabitEthernet6/0* and **ip access-group** *100* **in** would deny inbound IP traffic with a destination address of 3.1.x.x).

  – That same ACL is applied to outbound traffic on a port of a different 3-port Gigabit Ethernet line card in the same router, but MPLS is enabled on that port (for example, **interface** *GigabitEthernet1/0*, **ip access-group** *100* **out**, and **tag-switching ip**).

  – The same ACL is then removed from the inbound port (for example, **interface** *GigabitEthernet6/0* and **ip access-group** *100* **in**).

  This situation occurs even though an extended ACL should not affect outbound Multiprotocol Label Switching (MPLS) traffic. For the given example, the result is that although the ACL is no longer applied to the inbound port, outbound traffic with a destination address of 3.1.x.x is blocked even though MPLS tags are being applied to it.

  Workaround: Remove and then reapply the ACL to the outbound port. For example, enter the following global configuration commands:

  configure {**terminal**} **interface** *GigabitEthernet1/0* **no ip access-group** *100* **out exit exit**
  configure {**terminal**} **interface** *GigabitEthernet1/0* **ip access-group** *100* **out exit exit**

  After these commands are entered, MPLS-tagged outbound traffic will flow normally.

- CSCdr77367

  Multiprotocol Label Switching (MPLS) Traffic Engineering tunnels may fail temporarily if a link along the path from the tunnel head end to the tail end fails. This situation occurs even if there are alternate paths from the tunnel head end to the tail end with sufficient resources to support the

tunnel. While the tunnel is down, traffic may be dropped or may traverse normally routed, best-effort paths. The tunnels are normally restored within several seconds, but in some cases the tunnels may not be restored for several minutes.

This situation has occurred in Cisco IOS Release 12.0 S images that support MPLS Traffic Engineering and may occur in any release that supports MPLS Traffic Engineering. There is no workaround.

- CSCdr83367

  When you attempt to configure aal5nlpid encapsulation on an ATM linecard that does not support aal5nlpid encapsulation, a traceback message may be displayed.

  Workaround: Do not configure aal5nlpid encapsulation on ATM linecards that do not support aal5nlpid encapsulation.

- CSCdr92924

  If three Cisco 12000 series Gigabit Switch Routers (GSRs) that are using Frame Relay encapsulation connect to each other, and the middle router is configured with access lists, pings between the routers fail. There is no workaround.

- CSCdr96702

  A Cisco 7500/RSP series router that is running Cisco IOS Release 12.0(11)S3 may continually display the following error messages:

```
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
-Traceback= 6026E448 60600878 605F73A4 605F6F24 605F70B0 605F5A04 605F5E98 605F64D8
605F6630 60251FE4 60249398 6015A3D4 6015A5D0 6015B2D8 6015BD00 6015C830
%SYS-2-MALLOCFAIL: Memory allocation of 120 bytes failed from 0x60600870, pool
Processor, alignment 0
-Process= "<interrupt level>", ipl= 2
-Traceback= 6026CC0C 6026E6B8 60600878 605F73A4 605F6F24 605F70B0 605F5A04 605F5E98
605F64D8 605F6630 60251FE4 60249398 6015A3D4 6015A5D0 6015B2D8 6015BD00
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
-Traceback= 6026E448 60600878 605F73A4 60602210 605F713C 605F5A04 605F5E98 605F64D8
605F6630 60251FE4 60249398 6015A3D4 6015A5D0 6015B2D8 6015BD00 6015C830
%SYS-3-INVMEMINT: Invalid memory action (malloc) at interrupt level
-Traceback= 6026E448 60600878 605F73A4 60602210 605F713C 605F5A04 605F5E98 605F64D8
605F6630 60251FE4 60249398 6015A3D4 6015A5D0 6015B2D8 6015BD00 6015C830
%SYS-3-INVMEMINT: Invalid memory action (malloc) at int
```

  There is no workaround.

- CSCds00085

  The distributed Cisco Express Forwarding (dCEF) counter may stop functioning on a PA-MC-2T3+ Multichannel port adapter after provisioning and then deprovisioning channel groups. There is no workaround.

- CSCds05337

  When the OC-48 spatial reuse protocol (SRP) line card is configured with packet-switch ASIC (PSA) input access control lists (ACLs), PSA output ACLs, and tag switching, the line card might reload under some circumstances. Please note that configuring of input and output PSA ACLs at the same time is not a recommended configuration and such a configuration should be avoided whenever tag switching is implemented. There is no workaround.

- CSCds08358

  An Enhanced Gigabit Ethernet Interface Processor (GEIP+) sometimes returns a wrong card type on Simple Network Management Protocol (SNMP). The GEIP+ should return a value of 199, but in this situation, the GEIP+ returns a value of 427, which is the card type for a Gigabit Ethernet port adapter (PA-GE). There is no workaround.

- CSCds14076

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running the gsr-p-mz.120-11.5.S image with 4-Port OC-12 and OC-48 Packet-over-SONET (POS) line cards might experience a condition where the line protocol does not come up when PPP encapsulation and IP access lists are configured on the interface.

  Workaround: Use High-Level Data Link Control (HDLC) encapsulation and access lists, or use PPP encapsulation and remove IP access lists from the interface.

- CSCds16062

  When a link is added to a bundle from another port adapter while Distributed Multilink PPP (DML-PPP) is running, a Cisco 7500/RSP series router may reload, and the port adapter in the bay will be switched off. There is no workaround.

- CSCds23164

  A Cisco 7500 series router with a spatial reuse protocol (SRP) interface that is running distributed Cisco Express Forwarding (dCEF) might not correctly process the access control lists (ACLs) that are applied to the SRP interface.

  Workaround: Disable dCEF on the SRP interface by entering the **no ip route-cache distributed** interface configuration command, or run centralized CEF by using the **ip cef** global configuration command.

- CSCds29058

  A Cisco 12000 series Gigabit Switch Router (GSR) might reload unexpectedly if all Multiprotocol Label Switching Traffic Engineering (MPLS TE) tunnels are removed. This situation occurs under heavy load conditions (for example, when several thousand routes and several hundred TE tunnels are removed).

  Workaround: Allow a delay of a couple of seconds between tunnel removals.

- CSCds29675

  A Cisco 12000 series Gigabit Switch Router (GSR) with a single-port OC-48 Packet-over-SONET (POS) line card might reload with a software-forced crach on the line card if the line card is experiencing over 120 MB of traffic. There is no workaround.

- CSCds30121

  A Cisco 12000 series Gigabit Switch Router (GSR) with approximately 100 switched virtual circuits (SVCs) may stop sending data randomly across any SVC. This situation is accompanied by “encapsualtion error2” failure messages.

  Workaround: Remove the SVC from the map group, and add it back again.

- CSCds30651

  Writing to an AT Attachment (ATA) device might cause the device to become unusable and result in the following error message:

  ```
  ATA_Status time out waiting for 1
  ```

  There is no workaround.

- CSCds32423

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running the gsr-p-mz.12.0(10.3)S1 image reloads with the following error message when the **no aps protect** interface configuration command is entered:

  ```
  System returned to ROM by bus error at PC 0x60180B9C, address 0xD0D0D19
  ```

  There is no workaround.

- CSCds35017

  A Cisco 12000 series Gigabit Switch Router (GSR) might reload when a map list entry that was just configured is reconfigured. There is no workaround.

- CSCds39506

  A Cisco 7500 series router that is functioning as a Multiprotocol Label Switching (MPLS) Provider router and is running a release later than Cisco IOS Release 12.0(9.3)S might not be able to properly forward MPLS packets that are coming into the router and are meant to be going out the ATM PPP interface. This situation is typically observed as output drops on the ATM interface. There is no workaround.

- CSCds42864

  On a Cisco 12000 series Gigabit Switch Router (GSR), a limited number of virtual circuits are available to each virtual path identifier (VPI) for the single-port OC-12 ATM and 4-port OC-3 ATM line cards.

  Workaround: Enter the **atm vc-per-vp** interface configuration command to change the number of available virtual circuits.

- CSCds43793

  Multiprotocol Label Switching (MPLS) packets with valid labels that are received on an interface may be forwarded even though there is no MPLS application enabled on this interface. Only interfaces in the global routing table are affected; interfaces configured in a VPN routing or forwarding instance (VRF) are not affected. There is no workaround.

- CSCds45117

  A Cisco 7500 series router might experience a Versatile Interface Processor (VIP) reload when switching Multiprotocol Label Switching (MPLS) packets under certain conditions including, but not necessarily limited to, interface flaps on that VIP. There is no workaround.

- CSCds49736

  In a redundant topology including Packet-over-SONET (POS) IP and ATM Tagging (TC-ATM) links, a Cisco 12000 series Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0 S might experience problems with allocating tags on TC-ATM links when there are flapping links in the core. The adjacent routers might get out of sync in tag virtual circuit (TVC) allocation, or the traffic might be forwarded across a nonoptimal path.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCds50894

  A Cisco 12008 Gigabit Switch Router (GSR) might reload with a “SYS-3-BADMAGIC” error message after you upgrade from Cisco IOS Release 11.2(18)GS3 to Cisco IOS Release 12.0(11)S3. In this situation, the decode reveals that the reload occurred in validblock(). The router will appear to stabilize after one or two reloads. There is no workaround.

- CSCds54982

  The Cisco Express Forwarding (CEF) table does not get updated properly on the Gigabit Ethernet line card.

  Workaround: Enter the **clear ip cef** command in EXEC mode to refresh the CEF table.

- CSCds59194

  A Cisco router that is running Cisco IOS Release 12.0(12.3)S may experience problems passing non-Gigabit Route Processor (GRP)-sourced traffic out Packet-over-SONET (POS) line cards. When this situtation occurs, all traffic from external sources passing through the line card that is

experiencing this condition is dropped with no indication of the drop in the counters or any other indication of failure. Traffic that is generated by the GRP (for example, Internet Control Message Protocol (ICMP) packets, Border Gateway Protocol (BGP) traffic, and OSPF protocol traffic) passes under these circumstances.

Workaround: Reload the line card.

- CSCds66103

  On an 8-port OC-3 Packet-over-SONET (POS) line card, running traffic through an interface that is configured with Tag Switching and Per Interface Rate Control (PIRC) may result in the line card reloading. There is no workaround.

- CSCds66107

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(10)S or 12.0(10)S1 might experience Cisco Express Forwarding (CEF) inconsistencies when new subinterfaces are being added to a 1-port OC-12 line card. In this situation, the entries for the remote adjacencies of the new subinterfaces are missing, and an aggregate to null0 is used instead.

  Workaround: Enter the **clear cef linecard** command in EXEC mode.

- CSCds72867

  On a Cisco 7200 series router, the interface may stop receiving traffic under extreme loads on C7200-I/O-GE+E or C7200-I/O-2FE/E input/output controllers and on PA-2FE-TX or PA-2FE-FX port adapters. There is no workaround.

- CSCds73407

  A Cisco router may experience a number of problems if attempts are made to configure forward error correction (FEC) with a PA-2FEISL port adapter. There is no workaround.

TCP/IP Host-Mode Services

- CSCds43512

  A Cisco 12012 Gigabit Switch Router (GSR) might be stuck in an endless loop and send ACK packets to a Cisco 4700 router. This situation occurs when the Cisco 4700 router is being used as Telnet relay and about 4000 packets per second of inbound traffic are coming from a single Cisco 12012 GSR and there is one Telnet session from the UNIX box to the Cisco 4700 router, which has 6 outgoing Telnet sesions. In this situation, the UNIX box still reports the Telnet session to be established, but the process that owns it seems to be gone. There is no workaround.

Wide-Area Networking

- CSCdr55294

  An Intermediate System-to-Intermediate System (IS-IS) update might result in high CPU utilization that causes the ATM and Fast Ethernet (FE) interfaces to pause indefinitely. There is no workaround.

- CSCdr90335

  A Versatile Interface Processor (VIP) may reload during an online insertion and removal (OIR). This is a unique condition that can occur with large routing tables. There is no workaround.

- CSCds30456

  Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a Gigabit Ethernet Interface Processor (GEIP) may cause an "output stuck" condition and a complex restart. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(14)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(14)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdr52856

  Enabling Multiprotocol Label Switching Traffic Engineering (MPLS TE) tunnels on a Cisco 7507 router might result in a memory leak by the interprocess communication (IPC) Seat Manager process and a reload of the router if NetFlow and NetFlow Export are enabled on the router and the NetFlow Export packets are going out of the MPLS-TE tunnels.

  Workaround: Disable NetFlow Export by entering the **no ip flow-export** *ip-address udp-port* global configuration command.

- CSCds25135

  A Cisco Route Switch Processor 8 (RSP8) might reload at boot time because of an unexpected exception if a **boot host tftp:**[[[*//host*]/*directory-path*]/*filename*] configuration command is present in the startup configuration.

  Workaround: Change the URL syntax in the configuration command to use the IP address instead of the host name. For example, use **boot host tftp:**[[[*//a.b.c.d*]/*directory-path*]/*filename*].

- CSCds33629

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running the gsr-p-mz image of Cisco IOS Release 12.0(9.1)S might reload in telnetBLOCK() while closing an existing Telnet session. There is no workaround.

- CSCds34304

  A Cisco 7500/RSP series router might experience a software-forced reload when fair queueing is configured on more than 512 interfaces. There is no workaround.

- CSCds41795

  A Cisco AS5800 series universal access server may experience a bus error at les_ipfib_flow_switch along with spurious interrupts at the same process.

  Workaround : Disable flow switching by entering the **no ip route-cache flow** interface configuration command.

- CSCds58988

  A Cisco 7507 or 7513 router with dual Route Switch Processor 2s (RSP2s), RSP4s, RSP4+s or RSP8s, that is running any version of Cisco IOS between Cisco IOS Release 12.0(12.6)S and Cisco IOS Release 12.0(13.6)S1 inclusive, might reload repeatly during bootup and fail to boot. In this situation, messages similar to the following are displayed:

  ```
  SLOT 7 RSP is system master SLOT 6 RSP is system slave RSP4 platform with 131072 Kbytes
  of main memory
  ```

```
Self decompressing the image : ##################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
###################################### [OK]
Nested r4k_return_to_monitor call (2 times)
-Traceback= 0 60255640 60253FCC 6023D8D0 602D42F8 602D3A58 602E1C0C 602E0EBC 602D6360
Nested r4k_return_to_monitor call (3 times)
-Traceback= 0 602D43EC 602D3A58 602E1C0C 602E0EBC 602E1B3C 602E0EBC 602D6360
*** System received a Bus Error exception *** signal= 0xa, code= 0x8, context=
0x612b6780 PC = 0x602dab18, Cause = 0x20, Status Reg = 0x34008002 DCL Masked Interrupt
Register = 0x000000ff DCL Interrupt Value Register = 0x00000000 MEMD Int 6 Status
Register = 0x00000000
SLOT 6 RSP is system master SLOT 7 RSP is system slave RSP4 platform with 131072 Kbytes
of main memory
Found bootloader image - slot0:rsp-boot-mz_120-13_3_S.bin
Self decompressing the image : ##################################################
################################################################################
################################################################################
################################################################################
################## [OK]
Nested r4k_return_to_monitor call (2 times)
-Traceback= 0 60162EB8 60161844 6014B148 601E1B78 601E12D8 601EF48C 601EE73C 601E3BE0
Nested r4k_return_to_monitor call (3 times)
-Traceback= 0 601E1C6C 601E12D8 601EF48C 601EE73C 601EF3BC 601EE73C 601E3BE0
*** System received a Bus Error exception *** signal= 0xa, code= 0x8, context=
0x609fdbb0 PC = 0x601e8398, Cause = 0x20, Status Reg = 0x34008002 DCL Masked Interrupt
Register = 0x000000ff DCL Interrupt Value Register = 0x00000000 MEMD Int 6 Status
Register = 0x00000020
SLOT 6 RSP is system master SLOT 7 RSP is system slave RSP4 platform with 131072 Kbytes
of main memory
(repeats)
```

Workaround: Pull out the slave RSP to allow the router to boot only the master RSP. Reverting to a version of Cisco IOS earlier than Release 12.0(12.6)S will also alleviate this condition.

Interfaces and Bridging

- CSCds03961

  When a Cisco 7507 router with a Gigabit Ethernet Interface Processor (GEIP) installed in slot 5 and slot 6 is upgraded to Cisco IOS Release 12.0(11)S, the GEIP may experience a reload when it is booted.

  Workaround: Run Cisco IOS Release 11.1(33)CC to stabilize the router.

IP Routing Protocols

- CSCdr49641

  A Cisco router that is running Cisco IOS Release 12.0(10)S and that receives a large packet that was fragmented before receipt may display the following error message at the rendezvous point of a Multicast network that is running Protocol Independent Multicast (PIM) sparse mode:

  ```
  %PIM-5-REG_ENCAP_INVALID: Bad register from <IP-address> for (<IP-address>,
  <Class-D-IP-address>). Trace = ....
  ```

  Workaround: Send a mix of large and small packets from the source so that the source tree is set up correctly by the small packets between the first hop and the Route Processor (RP). If the Multicast data is forwarded correctly, then this situation may not cause any real harm.

  Alternate workaround: Reduce the packet size from the source so that fragmentation does not occur between the first hop and the RP.

- CSCdr50217

  Under rare circumstances, when a Cisco router does not receive any updates but has to send numerous updates to a peer router, Border Gateway Protocol (BGP) sends updates slowly because of a scheduling inefficiency in BGP. There is no workaround.

- CSCdr76940

  A Cisco 12000 series Gigabit Switch Router (GSR) might display the following error message:

  ```
  %LC-3-PSALOADSHARE MPLS loadsharing inconsistency for 0.0.0.0/0
  ```

  No other problems have been proven to be related to this message. If you see any MPLS load-sharing forwarding problems near the time the error message was displayed, contact your Cisco technical support representative. There is no workaround.

- CSCdr89108

  Multicast distributed switching (MDS) sometimes does not function properly on a Versatile Interface Processor (VIP) interface of a Cisco 7500/RSP series router; the interface is inadvertently changed to process switching when there are process switching interfaces in the router.

  Workaround: Reenter the **no shutdown** configuration command on the affected interfaces.

- CSCds05364

  When Distributed FRF.12 and Quality of Service (QoS) service policy are configured on a large number of Frame Relay permanent virtual circuits (PVCs), FRF.12 might not function after the router reloads. In this situation, the output of the **show frame-relay fragment** command will show no fragment count even though FRF.12 appears to be configured properly.

  Workaround: Reconfigure FRF.12 after the router reloads.

- CSCds11636

  Writing a configuration to NVRAM that contains “ip nbar resources” may cause A Cisco router to reload.

  Workaround: Do not save network-based application recognition (NBAR) resource configurations to NVRAM.

- CSCds12065

  A Cisco 12008 Gigabit Switch Router (GSR) that is running the gsr-k4p-mz image in Cisco IOS Release 12.0(11)S may display the following error message without any debugging enabled:

  ```
  %GRP-3-IFCON: TOO MANY QUEUED MESSAGES
  ```

  There is no workaround.

- CSCds20926

  A router that is running Open Shortest Path First (OSPF) may reload during redistribution testing. This situation has only been seen in development-testing environments, where different routing protocols are configured and unconfigured quickly. Race conditions occur if these protocols are redistributed into OSPF, which forces the router to reload. This situation does not occur in normal operating environments where routing protocols are never removed. There is no workaround.

- CSCds26009

  Using the **summary-address** router configuration command in Open Shortest Path First (OSPF) may cause high CPU utilization. This situation occurs if the routing table is 10K or above.

  Workaround: Remove the **summary-address** command.

- CSCds37837

  Rate-based distributed Quality of Service (QoS) features such as traffic-shaping, Low Latency Queueing (LLQ), and police do not report actually traffic rate after Compressed Real-Time Traffic Protocol (CRTP) has compressed the packets. This situation may result in premature packet drops.

  For example, if the compression efficiency is 2:1, and a given QoS feature has enough tokens for two compressed packets, instead of being able to send a burst of two voice packets, the feature may drop the second packet because it does not debit the tokens using the compressed size.

  There is no workaround.

- CSCds39722

  A Cisco router that has Cisco Express Forwarding (CEF) enabled may reload when sending NetFlow export packets. There is no workaround.

- CSCds44496

  A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

  The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flag is the extended length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). BGP uses the extended length bit only if the length of the attribute value is greater than 255 octets.

  An optional, transitive attribute that is unknown to a BGP speaker must be stored and forwarded when the path is sent in a BGP UPDATE. If the length of the attribute is such that the extended length bit is used, its contents are truncated when the UPDATE is sent. There is no workaround.

- CSCds53104

  A Cisco router may reload while changing an interface IP address if overlapping network statments exist in the OSPF configuration that match this IP address.

  Workaround: Remove extra network statements that match the old IP address.

Miscellaneous

- CSCdm62717

  A Cisco 12000 series Gigabit Switch Router (GSR) line card might reload if there are a large number of adjacency and prefix updates in a short period of time. This condition also affects Versatile Interface Processor (VIP) line cards in the Cisco 7500/RSP series routers.

  Workaround: Upgrade to Cisco IOS Release 12.1(10.5) or to a later release.

- CSCdr31064

  Under rare conditions, the Cisco 12000 series Gigabit Switch Router (GSR) switch fabric redundancy system may experience line card reloads and interprocess communction (IPC) errors while recovering from a Clock Scheduler Card (CSC) hardware failure. This problem is more frequent under high traffic load. There is no workaround.

- CSCdr61724

  Resolution of recursive routes by Cisco Express Forwarding (CEF) may add 1 to 15 seconds to the end-to-end route convergence time. There is no workaround.

- CSCdr62580

  When a Packet-over-SONET (POS) interface with an OC-48c/STM-16 POS line card on a Cisco 12008 series Gigabit Switch Router (GSR) is disconnected and then reconnected, the router may stop functioning and exhibit continuous "%LC-2-INTSCHED" and traceback output messages. This behavior may also occur when the other end of the POS line is a Cisco 12008 router that goes down/up. There is no workaround.

- CSCdr69544

  A Cisco 12016 or 12012 Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(9.6)ST2 with DC power displays might repeatedly display the following error messages:

  ```
  GSR_ENV-0-SHUTDOWN: Slot 24 Inlet sensor temperature at 33 deg C > 0 deg C
  GSR_ENV-0-SHUTDOWN: Slot 24 48V supply at 50V < 65408 V
  ```

  The router does not actually shut down, but the messages display repeatedly. This situation may also occur with a Cisco 12016 GSR with an AC power supply. There is no workaround.

- CSCdr72018

  When an OC-48c/STM-16c Packet-over-SONET (POS) line card is pulled from a Cisco 12000 series Gigabit Switch Router (GSR), no traps are generated. When the card is reseated, both LinkDown and LinkUp traps are received. When a Gigabit Ethernet (GE) card is pulled, no traps are generated, and when the card is reseated, only a LinkUp trap is received. There is no workaround.

- CSCdr84883

  Under certain circumstances when the access control list (ACL) matches the type of service (ToS) bits or Internet Control Message Protocol (ICMP) messages where the packet gets sent to the line card CPU for processing, the Multiprotocol Label Switching (MPLS) label imposition does not occur. The packet gets forwarded to the next hop as an IP packet rather than an MPLS packet. The router in the next hop puts an MPLS label on the packet. This situation does not affect packet flow; in the case of traffic engineering (TE) tunnels, the packet will be sent as IP and may not go through the TE tunnel. There is no workaround.

- CSCds01236

  A Cisco 7200 or 7500/RSP series router with an ATM-PA3 port adapter might stop forwarding packets on one or more virtual channels (VCs). In this condition, the packets show up as output drops on those VCs, and the VCs appear stuck.

  Workaround: Enter the **shutdown** configuration command followed by the **no shutdown** configuration command.

- CSCds04454

  A single-port Packet-over-SONET (POS) OC-48c/STM-16 Cisco 12000 series Gigabit Switch Router (GSR) Engine 2 line card may reload intermittently. There is no workaround.

- CSCds09570

  A Cisco 12000 Gigabit Switch Router (GSR) line card might reload if input MAC accounting is configured on a Gigabit Ethernet (GE) port on a 3-port GE line card. There is no workaround.

- CSCds11405

  When encapsulation Frame Relay is enabled on a Packet-over-SONET (POS) interface with multiple subinterfaces, the following error message may be seen in the log:

  ```
  SLOT 5:21:43:50: %LC-3-OUTINFO: Adj/midb(MDS 224.0.0.2): incorrect output_info=0
  -Traceback= 40318D38 40368518 403643AC 403666C4 403667B0 40365F88 4009C074 40090 Slot
  5 is where the OC3 is doing frame relay encapsulation.
  ```

  There is no workaround.

- CSCds12065

  A Cisco 12008 Gigabit Switch Router (GSR) that is running the gsr-k4p-mz image in Cisco IOS Release 12.0(11)S may display the following error message without any debug enabled:

  ```
  %GRP-3-IFCON: TOO MANY QUEUED MESSAGES
  ```

  There is no workaround.

- CSCds12078

  A Cisco 7200 series router with a NPE-200 Network Processing Engine and a PA-2FEISL port adapter might experience spurious memory access while Cisco Express Forwarding (CEF) is enabled.

  Workaround: Disable CEF.

- CSCds13541

  Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic may be dropped in a Provider core network that has MPLS traffic engineering tunnels configured. This situation occurs when the dropped traffic follows a path through the core network that traverses an MPLS traffic engineering tunnel interface on which IP Label Switching has been configured. This situation only occurs on Cisco routers that are running Cisco IOS Release 12.0 S and acting as MPLS Traffic Engineering (TE) head end routers that are carrying packets that are already labeled, such as MPLS VPN traffic.

  Workaround: After a traffic engineering tunnel interface comes up on a Provider core router, enter the following command sequence:

  configure terminal

  interface Tunnel *tunnel-number*

  no tag-switching ip

  tag-switching ip

- CSCds16875

  Traffic might fail to be forwarded into Multiprotocol Label Switching (MPLS) tunnels after the tunnel has been dynamically rerouted. There is the possibility that after the tunnel has been rerouted to a different interface, probably because of a change in the network topology, that traffic might be lost when forwarded to the tunnel.

  Workaround: Shutdown the tunnel interface by entering the **shutdown** command and then bring up the interface a few seconds later by entering the **no shutdown** command.

- CSCds16953

  After a microcode reload, packets that are traveling through a Cisco 7500/RSP series router may get process-switched instead of getting distributed Cisco Express Forwarding (dCEF)-switched. This situation impacts the performance of the router. If the packets get process-switched while Distributed Multilink PPP (DML-PPP) is running, CPU utilization may reach close to 100 percent with 5 to 6 T1s. There is no workaround.

- CSCds16995

  On a Cisco 7500/RSP series router, if you deconfigure a link from a bundle while Distributed Multilink PPP (DML-PPP) is running and the link is assigned an IP address, pings through this link fail. In this situation, the link that has been deconfigured can no longer carry traffic.

  Workaround: Deconfigure the whole bundle and then reconfigure the bundle without this link. After you perform this action, the link should function properly.

- CSCds17239

  If a Cisco 12000 series Gigabit Switch Router (GSR) is configured with access control lists (ACLs) that are longer than 128 lines, and these ACLs are applied inbound on an Engine 2 (PSA-based) line card interface, traffic that is destined for the router may be dropped. This situation applies to traffic such as Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), and routing protocol updates.

  This situation is seen only on Engine 2 (PSA) line cards, and only when an ACL longer than 128 lines is applied inbound. No other configurations are vulnerable to this defect. There is no workaround.

- CSCds17914

  File operations may be erratic if you have a corrupted file on either a Personal Computer Memory Card International Association (PCMCIA) Flash memory card or a SanDisk PCMCIA card, and you try to do something with the file such as copy it or delete it. There is no workaround.

- CSCds18648

  Policy routing on Cisco 12000 series Gigabit Switch Router (GSR) does not function properly for IP option packets and may cause a line card reload. There is no workaround.

- CSCds19179

  If the first interface in FlexWAN does not have the **route-cache flow** command configured and you try to configure **route-cache flow** for later interfaces on that slot, it might cause a reload during online insertion and remoal (OIR) operations.

  Workaround: Enter the **route-cache flow** interface configuration command on the first interface of a port adapter.

- CSCds20491

  A Cisco router that is running Cisco IOS Release 12.0(11.6)ST reloads when you use a load balancing route discovery command with a VPN routing/forwarding (VRF) instance specified (for example, the **show ip cef vrf** [*vrf*] **exact-route** [*src-addr*] [*dest-addr*] EXEC command). There is no workaround.

- CSCds21333

  Some quality of service (QoS) features may not perform as expected when Cisco Express Forwarding (CEF) is enabled. There is no workaround.

- CSCds21669

  If a Cisco 7500/RSP series router is booted with Multilink PPP (MLPPP) running and then distributed Cisco Express Forwarding (dCEF) switching is enabled after the router comes up, distributed MLPPP (DMLPPP) does not come up. In this situation, packets will not be distribute switched. Instead, the switching would be done by the RSP depending on the type of switching that is configured. There is no workaround.

- CSCds21813

  A Cisco 12000 series Gigabit Switch Router (GSR) might experience spurious accesses when switching IP packets if features like access lists are enabled. There is no workaround.

- CSCds26361

  A Cisco 12000 series Gigabit Switch Router (GSR) might access a NULL pointer and experience a memory fault reload if the router runs out of memory and tries to increase the size of the Multiprotocol Label Switching Traffic Engineering (MPLS TE) maximum link-state advertisement (LSA) received. There is no workaround.

- CSCds27045

  The **atm sonet stm-4** interface configuration command is added to the configuration automatically when upgrading to Cisco IOS Release 12.0(12)S or 12.0(12.6)S. Removing this line in the configuration of a Cisco 12000 series Gigabit Switch Router (GSR) results in an error. On a Cisco 7500/RSP series router, the **atm sonet stm-4** command cannot be removed from the configuration. There is no workaround.

- CSCds27443

  Configuring Cisco Express Forwarding (CEF) is configured on a Cisco 7200 series router might cause a 50 percent packet loss.

  Workaround: Clear the Address Resolution Protocol (ARP), or clear the adjacencies.

- CSCds31512

  IP option packets may cause Cisco 12000 series Gigabit Switch Router (GSR) line cards to reload if policy routing is enabled. This situation occurs only when the GSR is running Cisco IOS Release 12.0(12.x) images. There is no workaround.

- CSCds32139

  A Cisco 12008 router that is running Cisco IOS Release 11.2(19)GS4.1 may reload with a bus error. There is no workaround.

- CSCds34124

  In Cisco IOS software that is running Multiprotocol Label Switching (MPLS)/Tag switching over ATM interfaces, virtual circuit (VC) resource exhaustion at the ATM driver level is not reported to the MPLS application during Label VC (LVC) creation. This situation causes MPLS to behave as

though it successfully created an LVC when the ATM driver actually failed to complete the request. The output of the **show atm vc** privileged EXEC command shows the LVC in the INACTIVE state, so the destination cannot be pinged over the affected LVC.

This situation occurs only when you set the virtual path identifier (VPI) or virtual channel identifier (VCI) label range negotiated during Label Distribution Protocol (LDP)/Tag Distribution Protocol (TDP) session establishment larger than the VC range of the interface and when all the VC resources on the interface are exhausted.

This situation usually does not occur when the ATM interface is connected to a BPX, IGX, MGX, or any ATM switch, because the VC resources are constrained by the ATM switch during label range negotiation.

Workaround: Set the label range to be smaller than the VC space to ensure that this condition never occurs.

- CSCds36057

  A Cisco 7500/RSP series router with a Versatile Interface Processor 4 (VIP4) and a PA-MC-2T3+ multichannel port adapter might reload after the **shutdown** interface configuration command is entered on a Multilink interface followed by the **no shutdown** interface configuration command. There is no workaround.

- CSCds36165

  On a Cisco 12000 series Gigabit Switch Router (GSR), Per Interface Rate Control (PIRC) may not function properly on Engine 2-based Packet-over-SONET (POS) line cards. There is no workaround.

- CSCds39861

  Multiprotocol Label Switching (MPLS) ATM Tag Distribution Protocol (TDP) bindings may not reestablish when TDP adjacencies flap. This situation may occur under high CPU utilization or when TDP neighbor adjacencies flap. This situation has been observed only when the TDP neighbor is running Cisco IOS Release 12.0(10)S or an earlier release. You can diagnose this problem by using the **show tag-switching atm-tdp bindings** privileged EXEC command. The symptoms are that the LER will have a tag ATM binding for a destination prefix while the downstream router will not. There is no workaround.

- CSCds43008

  On a Cisco 7200 series router, if a policy map is configured with multiple classes and attached to an interface, the following error messages might be displayed after the configuration is saved in NVRAM and the router is reloaded:

  ```
  class d1 ^ % Invalid input detected at '^' marker.
  class q1 ^ % Invalid input detected at '^' marker.
  ```

  Workaround: Reconfigure the policy map after the router is reloaded.

- CSCds44514

  A Cisco 12000 series Gigabit Switch Router (GSR) may display messages similar to the following message if the router is configured with access control lists (ACLs) that use the "log-input" keyword on gigabit or Fast Ethernet interfaces:

  ```
  %ALIGN-3-TRACE: -Traceback= 4036C724 402D9A38 4031B8D0 400BA094 00000000 00000000
  00000000 00000000
  ```

  Workaround: Remove the "log-input" keyword in the ACL definition.

- CSCds46872

  Configuring IP accounting on a Cisco 12000 series Gigabit Switch Router (GSR) by entering the **ip accounting** interface configuration command halts all traffic through the router. This situation does not occur if the **ip accounting mac-address** command is used.

  Workaround: Use the **ip accounting mac-address** command.

- CSCds49677

  The number of adjacencies a Gigabit Ethernet line card will support in this release is 32k without 802.1Q and 21k with 802.1Q. If this number of adjacencies is exceeded, the router displays error messages similar to the following:

  ```
  GRP-3-ENCAP: Failure to allocate, slot X (info 0x22)
  ```

  You can see the number of adjacencies by entering the **show adjacency** [**summary**] command. Entering the **clear arp** command normally reduces the number of adjacencies until each end device is required through ARP. There is no workaround.

- CSCds55488

  Multiprotocol Label Switching (MPLS) ATM Tag Distribution Protocol (TDP) bindings may continuously flap between active and released states under certain stressful situations when Cisco IOS Release 12.0(13)S or previous versions of Cisco IOS Release 12.0 S are running. There is no workaround.

- CSCds58727

  On a Cisco 7513 router, pings may fail through Multiprotocol Label Switching Traffic Engineering (MPLS TE) unidirectional tunnels when Cisco Express Forwarding (CEF) is configured. There is no workaround.

- CSCds61573

  When an OC-3 ATM line card is configured with the egress Committed Access Rate (CAR), traffic is not forwarded if the receive (Rx) line card is a 3-port Gigabit Ethernet line card. There is no workaround.

- CSCds69928

  On a Cisco 7500/RSP series router that is running Cisco IOS Release 12.0(13.6)S or 12.0(13.6)S1, when a service policy is attached to an ATM or Frame Relay VC, class-map statistics are correct, but feature statistics (for example, bandwidth or polic) are all zeros.

  Workaround: Attach a service policy to ATM or Frame Relay subinterfaces.

TCP/IP Host-Mode Services

- CSCdk69541

  If a Cisco router is running Cisco IOS Release 12.0 S and the “ip tcp path-mtu-discovery” feature is enabled, the router might experience a TCP timer problem and reload. This situation occurs when the router is experiencing a heavy load that includes a large number of Border Gateway Protocol (BGP) peer routers that are exchanging routing packets.

  Workaround: Disable the "ip tcp path-mtu-discovery" feature by entering the **no ip tcp path-mtu-discovery** command.

Wide-Area Networking

- CSCds30986

  Both 2x32-bit and 64-bit counters are incorrect when using Packet-over-SONET with Frame Relay encapsulation on subinterfaces. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(13)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(13)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdm56157

  A Cisco Route Switch Processor (RSP) might periodically display the following traceback:

  ```
  IPC-5-INVALID: Sequence Structure port index=0x0 appears on the console.
  ```

  When you enable the **debug ipc errors** EXEC command, the RSP might display the following traceback:

  ```
  IPC: SEQ_ERR ACK ... source seat 0x1000000 port 0x0
  ```

  If you enter the **show ipc stat** command, the RSP produces “messages dropped on input” and “no local port” errors.

  This situation might occur when distributed Cisco Express Forwarding (dCEF) is enabled on line cards. There is no workaround.

- CSCdr54711

  On a Cisco router that is running Cisco IOS Release 12.0(10)S, aggregate NetFlow might report the -cef layer ifIndex related to the physical interface instead of reporting the actual physical interface ifIndex. There is no workaround.

- CSCdr71374

  When output access control lists (ACLs) are configured on a Cisco 12000 series Gigabit Switch Router (GSR) with Performance-48 or 3-Port Gigabit Ethernet line cards, packets that have a tag imposed on them by these cards may be transmitted with the incorrect tag Time to Live (TTL). There is no workaround.

- CSCdr77460

  When an online insertion and removal (OIR) is performed, the IF-MIB ifTable, ifStackTable, and ifNumber retains the old entries even though the associated interface layers have been removed. There is no workaround.

- CSCdr90474

  On a Cisco router that is running Cisco IOS Release 12.0(11.6)S, 64-bit Simple Network Management Protocol (SNMP) counters might count backwards for in/out octets on idle Ethernet interfaces. There is no workaround.

- CSCdr93938

  The ifHCInOctets counter might report incorrect values during reloads for a Packet-over-SONET (POS) interface on a Cisco 12000 series Gigabit Switch Router (GSR). There is no workaround.

EXEC and Configuration Parser

- CSCdr53609

  Deleting one serial subinterface from the running configuration on a Cisco 7500/RSP series router with a Route Switch Processor 4 (RSP4) that is running Cisco IOS Release 12.0(9)S or 12.0(10.3)S1 will cause the whole interface to disappear.

  Workaround: Add the interface that was deleted back to the configuration.

Interfaces and Bridging

- CSCds12978

  On a Cisco 7200 series router, the High-Level Data Link Control (HDLC) encapsulated interface on a Packet-Over-SONET (POS) port adapter is never up after reloading unless you configure the **cdp enable** or **clock source internal** interface configuration commands.

  Workaround: Use the **clear interface** EXEC command or a sequence of the **shut** and **no shut** interface commands.

IP Routing Protocols

- CSCdr49641

  A Cisco router that is running Cisco IOS Release 12.0(10)S and receives a large packet that was fragmented before receipt might display the following error message at the rendezvous point of a multicast network that is running PIM sparse mode:

  ```
  %PIM-5-REG_ENCAP_INVALID: Bad register from <IP-address> for (<IP-address>,
  <Class-D-IP-address>). Trace = ....
  ```

  There is no workaround.

- CSCdr68435

  If the **set interface** route-map configuration command is entered on a Cisco router that is using distributed policy routing, the subinterfaces do not function properly, and the command will not work on an interface that is on a different line card.

  Workaround: Enter the **set ip next-hop** route-map configuration command rather than the **set interface** command.

- CSCdr88511

  A Cisco router that is running Cisco IOS 12.0(10.6)S2 or later releases might not install default routes that are advertised though type 5 link-state advertisements (LSAs) by other routers. This condition occurs when the Cisco router has only type 5 default LSAs and no nondefault type 5 LSAs are present in the database.

  Workaround: Add a nondefault external LSA to the database.

- CSCdr89108

  Multicast distributed switching (MDS) does not function properly on ATM subinterfaces on Cisco 7500/RSP series routers. Instead of being switched by the Versatile Interface Processor (VIP), the multicast traffic in this situation will be sent to the Route Switch Processor (RSP) to be switched by the RSP CPU.

Temporary workaround: Remove the incoming ATM subinterface, and then add a new subinterface that has the same configuration. (See the following example, in which multicast traffic comes in at ATM4/1/0.3.) This action will cause MDS to function normally and the switching to be performed by the VIP. Please note, however, that once the router is rebooted, MDS will start to fail again.

```
!
interface ATM4/1/0.3 point-to-point
ip address 192.168.100.1 255.255.255.0
no ip directed-broadcast
ip pim dense-mode
atm pvc 3 0 300 aal5snap
no atm enable-ilmi-trap
!


Router#conf t
```

Note Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#no interface atm4/1/0.3
```

Note Not all configurations will be removed; they may reappear after the subinterface has been reactivated.

```
Router(config)#interface atm 4/1/0.4 point-to-point
Router(config-subif)# ip address 192.168.100.1 255.255.255.0
Router(config-subif)# no ip directed-broadcast
Router(config-subif)# ip pim dense-mode
Router(config-subif)# atm pvc 3 0 300 aal5snap
Router(config-subif)# no atm enable-ilmi-trap
Router(config-subif)#no shut
Router(config-subif)#^Z
Router#
```

- CSCdr90410

  Static routes that are within the range of a network statement where the gateway is an interface will not be distributed into OSPF by the **redistribute static** command.

  Workaround: Do not cover static to the interface by the network statement under OSPF.

Miscellaneous

- CSCdm62717

  A Cisco 12000 series Gigabit Switch Router (GSR) line card might reload if there is a large number of adjacency and prefix updates in a short period of time. This condition also affects Versatile Interface Processor (VIP) line cards in the Cisco 7500/RSP series routers.

  Workaround: Upgrade to Cisco IOS Release 12.1(10.5) or later release.

- CSCdm88828

  Multiprotocol Label Switching (MPLS) with redundant parallel links may fail in certain cases.

  Workaround: Upgrade to Cisco IOS Release 12.0(13)S.

- CSCdr02061

  On the output Versatile Interface Processor (VIP) interfaces of a Cisco 7500/RSP that is running Cisco IOS Release 12.0 S, Multiprotocol Label Switching (MPLS) packets are not classified correctly for Distributed Weighted Random Early Detection (DWRED) and Distributed Weighted Fair Queueing (DWFQ). In this situation, all MPLS packets will be considered class 0 by these algorithms regardless of the actual value of their MPLS experimental field values. There is no workaround.

- CSCdr03956

  A Cisco 7200 series router running Cisco IOS Release 12.0(7)XE1 with multicast and tunneling configured on a PA-A3-8T1 IMA port adapter may reload due to a software forced reload caused by a memory corruption problem. There is no workaround.

- CSCdr06072

  Multicast forwarding might stop for a specific group on the outgoing interface for a given multicast client if the client is pruned after leaving the group and later joins the group again. This condition occurs only in Protocol Independent Multicast (PIM) dense mode; PIM sparse mode is not effected.

  Workaround: Clear the multicast route for the group for that client by entering the **clear ip mroute** {*group*} command.

- CSCdr13521

  A low memory condition might provoke a reload in Integrated File System (IFS). There is no workaround.

- CSCdr35715

  Under certain circumstances, a Cisco router may reload when crypto is enabled on a FDDI.

  Workaround: Disable Cisco Express Forwarding (CEF) on the affected interface.

- CSCdr37306

  When a Multiprotocol Label Switching (MPLS) tunnel is created on a Cisco 12000 series Gigabit Switch Router (GSR), and this tunnel goes out over a Packet-over-SONET (POS) interface, traffic that is routed from an incoming line card into the tunnel has a corrupted frame header, which causes the frame to be discarded.

  Workaround: Ensure that tag switching is enabled by entering the **tag-switching ip** interface configuration command.

- CSCdr48014

  Open Shortest Path First (OSPF) updates may be corrupted on a Cisco 7500 series router using Multiprotocol Label Switching (MPLS) switching with Cisco Express Forwarding (CEF) output features enabled (including “service policy output”). IP routes are temporarily deleted from the IP routing table, and a loss of connectivity may occur.

  Workaround: Configure the **ip cef** global configuration command. Then execute the **copy running start** command, and reload.

  Alternative workaround: Enter the **memory cache-policy io uncached** command. However, entering this command might sacrifice packet switching performance.

- CSCdr49537

  The five-minute output rate counters on a PA-MCT3 interface may not match the five-minute input rate of the directly connected serial interface. There is no workaround.

- CSCdr49601

  A Gigabit Ethernet Interface Processor (GEIP) on a Cisco 7500 series router may experience receiving problems that cause the router to pause indefinitely.

  Workaround: Disable dCEF on the GE interface.

- CSCdr57631

  If both access control lists (ACLs) and Multiprotocol Label Switching (MPLS) are configured on a Cisco 12000 series Gigabit Switch Router (GSR) with a 3-Port Gigabit Ethernet line card, traffic may not pass through that interface. There is no workaround.

- CSCdr62168

  Upon system initialization, ATM permanent virtual circuits (PVCs) are left in the inactive state and do not change to the active state unless the user issues a shutdown/no shutdown of the associated ATM interface in configuration mode.

  Workaround: Reinitialize the interfaces manually.

- CSCdr65006

  A Cisco 12000 series Gigabit Switch Router (GSR) may fail to properly forward Multiprotocol Label Switching (MPLS)-encapsulated frames over Gigabit Ethernet line cards. In this condition, the traffic sent on to a tunnel head over the Gigabit Ethernet interface is dropped, and any MPLS-encapsulated frame forwarded by the GSR over a Gigabit Ethernet line card is sent with an invalid or garbled destination MAC address and is not received. There is no workaround.

- CSCdr65544

  A Versatile Interface Processor (VIP) may reload after fragmenting packets if distributed Cisco Express Forwarding (dCEF) is enabled. The same condition may occur with a Cisco 7200 series router if CEF is enabled. There is no workaround.

- CSCdr67801

  A Cisco 7200 series router or a Cisco 7500/RSP series router with a PA-A3 ATM port adapter may reload because of a bus error that points to an 0x50000000 address or an 0x08000000 address. These reloads occur after the PA-A3 driver has received a packet and attempts to process it.

  Workaround: Disable Cisco Express Forwarding (CEF) by entering the **no ip cef** global configuration command on the Cisco 7200 series router or by entering the **no ip cef** [**distributed**] global configuration command on the Cisco 7500/RSP series router.

- CSCdr68932

  Configuring an output access control list (ACL) on a Cisco 12000 series Gigabit Switch Router (GSR) with a 3-Port Gigabit Ethernet line card may result in the reload of the 3-Port Gigabit Ethernet line card if the line card is also performing tag imposition and the ACL contains a rule regarding the packet's source port, type of service, precedence, logging, or Internet Group Management Protocol (IGMP). There is no workaround.

- CSCdr75997

  CSCdm94333, which was integrated in Cisco IOS Release 12.0(9.6)S, introduced a new version of the automatic protection switching (APS) protect group protocol that required both working and protect routers to be upgraded simultaneously. The fix for CSCdr75997 relaxes this restriction by supporting interoperability between systems that are running different versions of the APS protocol so that working and protect can be upgraded independently.

- CSCdr77472

  When an online insertion and removal (OIR) is performed for a Switch Fabric Card (SFC) or Clock and Scheduler Card (CSC) for a Cisco 12000 series Gigabit Switch Router (GSR), the OLD-CISCO-CHASSIS-MIB and ENTITY-MIB do not reflect this OIR event, and a card that has been removed still appears in both MIBs. There is no workaround.

- CSCdr80686

  When a rate-limiting feature (for example, committed access rate (CAR)) or a QoS feature (for example, access-control list (ACL)) is enabled on an interface of an Engine 0 or Engine 1 line card on a Cisco 12000 series Gigabit Switch Router (GSR), the receive (RX) byte and packet counters for that interface shows the net number of byte and packets that have been admitted to the interface. In this situation, packets that are dropped at the interface because of CAR or ACL are excluded from the RX byte and packet counters. There is no workaround.

- CSCdr80820

  A Cisco 12000 series Gigabit Switch Router (GSR) that is configured for distributed IP multicast might exhibit the following error messages:

  ```
  SLOT 8:03:43:10: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x402EB90C reading
  0x0
  SLOT 8:03:43:10: %ALIGN-3-TRACE: -Traceback= 402EB90C 402E779C 402E9AC4 402E9BA8
  402E9388 4009B02C 4009B018 00000000
  SLOT 8:03:43:10: %ALIGN-3-TRACE: -Traceback= 402EB910 402E779C 402E9AC4 402E9BA8
  402E9388 4009B02C 4009B018 00000000
  ```

  There is no workaround.

- CSCdr81857

  If a QoS service-policy is configured on a channelized interface on a PA-MC-T/E1 or PA-MC-T/E3 port adapter, entering the **microcode reload** global configuration command under heavy traffic might result in a failure to forward packets for the interface.

  Workaround: Remove the service-policy before entering the **microcode reload** command, and then reapply the policy.

- CSCdr83067

  If the **clear counters** EXEC command is entered from a Secure Shell (SSH) connection on a router with E1/T1 controllers, a "SYS-3-CPUHOG" error message might be exhibited. This condition occurs when the **clear counters** command fails on more than one E1/T1 controller with a "POT1E1-3-MBOXSEND" error.

  Workaround: Clear each E1/T1 controller individually.

- CSCdr83141

  Under certain circumstances, configuration on an ATM permanent virtual connection (PVC) might fail with the following error message:

  ```
  ATM hardware failed cannot update vc
  ```

  If Operation, Administration, and Maintenance (OAM) is also configured, the router might reload after the error.

  Workaround: Do not enter the **show policy interface** global configuration command.

- CSCdr88949

  The performance rate after traffic shaping on four-port OC-3 and single-port OC-12 line cards on Engine 0 may degrade if distributed traffic shaping (DTS) is configured. There is no workaround.

- CSCdr90642

  On Engine 0 card, the Weighted Random Early Detection (WRED) queue average and drop counter calculations might not be accurate because process timer expiration might vary under the packet-handling load. Under traffic loads that do not respond to drops (for example, User Datagram Protocol (UDP) or load generator), there might be short periods of time where the link bandwidth drops to 0 bps. In this situation, every packet might be dropped. There is no workaround.

- CSCdr91303

  When attaching and removing a QoS service-policy under a heavy traffic load on a channelized interface on a MC-T/E1 or MC-T/E3 port adapter, packets might stop forwarding out of the interface.

  Workaround: Enter the **microcode reload** global configuration command.

- CSCdr91482

  The Cisco 12000 series Gigabit Switch Router (GSR) will incorrectly increment the input drops counter because of an accounting issue. This action might not correctly reflect packets dropped because of congestion. This situation might be seen on all GSR interfaces, but has no effect on service or functionality of the interfaces. There is no workaround.

- CSCdr95090

  When a policy map is attached to an interface on a Cisco 7200 series router, the router experiences spurious memory access at the function hqf_get_policymap(). There is no workaround.

- CSCds02168

  Entering the **show ip cache flow** EXEC command on the line card of a Cisco 12000 series Gigabit Switch Router (GSR) might cause null destination interfaces to be reported in exported packets and the output of the **show ip cache flow** command if output Committed Access Rate (CAR) is enabled.

  Workaround: Remove output CAR.

- CSCds06676

  On a Cisco 7200 series router that is running Cisco IOS Release 12.0(12)S with Dynamic Packet Transport (DPT), the Intelligent Protection Switching (IPS) packets that are sent by the node have a MAC address of 0000.0000.0000, which results in instability on the DPT ring.

  Workaround: Manually configure a MAC address on the DPT interface.

- CSCds08615

  All packets that are received on an interface with an access control list (ACL) applied that is supposed to be processed by the packet-switched ASIC (PSA) might actually be processed by the CPU. This situation occurs only with interfaces other than interface 0 on the card. This condition results in lower performance for the packets that are received on these interfaces. There is no workaround.

- CSCds10029

  Removing a service policy from a large number of Frame Relay permanent virtual circuits (PVCs) might prevent packets from being forwarded out of the entire interface. The commands that lead to this situation are:

  interface *s1/00:0*
  no frame-relay class *name*

  or

  map-class frame-relay *map-class name*
  no service-policy {**output**} *policy-map*

  Workaround: Attach a dummy Class-Based Weighted Fair Queueing (CBWFQ) policy to the interface, and then remove the policy.

- CSCds11189

  Low Latency Queueing (LLQ) and Class-Based Weighted Fair Queueing (CBWFQ) do not function properly on an ATM subinterface policy after that interface has been brought down and up or if the link flaps.

  Workaround: Apply the service policy under the permanent virtual connection (PVC). In this situation, the policy functionality is not affected by link flaps.

  Alternate Workaround: Reattach the subinterface service policy after the interface or link comes up.

- CSCds12078

  A Cisco 7200 series router with a NPE-200 Network Processing Engine and a PA-2FEISL port adapter might experience spurious memory access while Cisco Express Forwarding (CEF) is enabled.

  Workaround: Disable CEF.

- CSCds13541

  Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) traffic may be dropped in a Provider core network that has MPLS traffic engineering tunnels configured. This situation occurs when the dropped traffic follows a path through the core network that traverses a MPLS traffic engineering tunnel interface on which IP Label Switching has been configured. This situation only occurs on Cisco routers that are running Cisco IOS Release 12.0 S and acting as MPLS Traffic Engineering (TE) head end routers that are carrying packets that are already labeled, such as MPLS VPN traffic.

  Workaround: After a traffic engineering tunnel interface comes up on a Provider core router, enter the following command sequence:

  – **configure terminal interface tunnel** *tunnel-number*
  – **no tag-switching ip**
  – **tag-switching ip**

- CSCds13547

  When Output Rate Limiting is configured on a Versatile Interface Processor (VIP) interface and the router is reloaded, the Rate Limiting functionality will not be properly enabled, and the Distributed Committed Access Rate (DCAR) functionality does not take effect.

  Workaround: Disable and then reenable the **rate-limit** interface configuration command.

- CSCds16995

  On a Cisco 7500/RSP series router, if you deconfigure a link from a bundle while Distributed Multilink PPP (DML-PPP) is running and the link is assigned an IP address, pings through this link will fail. In this situation, the link that has been deconfigured can no longer carry traffic.

  Workaround: Deconfigure the whole bundle and then reconfigure the bundle without this link. After you perform this action, the link should function properly.

- CSCds17239

  If a Cisco 12000 series Gigabit Switch Router (GSR) is configured with access control lists (ACLs) that are longer than 128 lines, and these ACLs are applied inbound on an Engine 2 (PSA-based) line card interface, traffic that is destined for the router may be dropped. This situation applies to traffic such as Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), and routing protocol updates.

  This situation is seen only on Engine 2 (PSA) line cards, and only when an ACL longer than 128 lines is applied inbound. No other configurations are vulnerable to this defect. There is no workaround.

TCP/IP Host-Mode Services

- CSCds13972

  Border Gateway Protocol (BGP) sessions on Cisco 12000 series Gigabit Switch Router (GSR) might fail to send updates when the router establishes passive BGP sessions because of problems with the flow control of BGP and TCP.

  Workaround: Use an inbound Access Control List (ACL) to deny any traffic destined for the port, and always open the session actively.

Wide-Area Networking

- CSCdr68102

  PA-A1 port adapters do not function when installed in bay 1 of a Versatile Interface Processor 4 (VIP4).

  Workaround: Install PA-A1 port adapters in bay 0 of VIP4s.

Resolved Caveats—Cisco IOS Release 12.0(12)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(12)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdp97532

  Snmpboots, a boot counter for SNMP Version 3, is incremented and saved during bootup, which might cause a noticeable bootup delay. This bootup delay will occur only when SNMP Version 3 is configured. There is no workaround.

- CSCdr59243

  A Cisco 7500 series router with a PA-CT3 port adapter that has been channelized down to a T1 might exhibit the following error messages on any of the channelized interfaces:

  ```
  %RSP-3-RESTART: cbus complex
  %RSP-3-RESTART: interface Serial5/0/0:1, output stuck
  ```

  In this condition, the channelized interfaces might enter a down/down state.

  Workaround: Reload the router.

- CSCdr77460

  When an online insertion and removal (OIR) is performed, the IF-MIB ifTable, ifStackTable, and ifNumber retains the old entries even though the associated interface layers have been removed. There is no workaround.

Interfaces and Bridging

- CSCdr16853

  A single Packet-over-SONET (POS) port adapter in a Cisco 7500/RSP series router with a Versatile Interface Processor 4 (VIP4) might stop transmitting and cause an “output stuck” condition. A POS port adapter that is a coresident with another port adapter in a Versatile Interface Processor 2 (VIP2) might also cause an “output stuck” condition for itself or the coresident port adapter. There is no workaround, but disabling distributed Cisco Express Forwarding (dCEF) globally, or in some conditions on the POS interface, will stop this condition from appearing.

IP Routing Protocols

- CSCdr45483

  A Cisco router with multicast configured might reload with a bus error if there are severe unicast route updates. There is no workaround.

- CSCdr88511

  A Cisco router that is running Cisco IOS 12.0(10.6)S2 or later releases might not install default routes that are advertised though type 5 link-state advertisements (LSAs) by other routers. This condition occurs when the Cisco router has only type 5 default LSAs and no nondefault type 5 LSAs are present in the database.

  Workaround: Add a nondefault external LSA to the database.

Miscellaneous

- CSCdm87756

  In a network where there are multiple paths between two networks and the paths travel through different sets of routers between these networks, per-destination load balancing will not be effective in any router after the first router where the load balancing paths diverge.

  Workaround: Use per-packet load balancing.

- CSCdp34901

  Entering the **clear ip rtp header-compression** EXEC command on a Frame Relay interface that has data-link connection identifiers (DLCIs) with no compression configured might cause the router to reload.

  Workaround: Do not enter the **clear ip rtp header-compression** command under these conditions.

- CSCdp42210

  A node route processor (NRP) ATM interface stops sending when there are multiple particles with data-length 0 at the last particle. The only way to exit out of this situation is to use the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command. There is no workaround.

- CSCdp67380

  A Cisco router might reload if the **show ip cef** EXEC command is entered while the routing table is changing. There is no workaround.

- CSCdp88625

  Under rare circumstances, a permanent virtual circuit (PVC) on a Cisco 6400 series node route processor (NRP) might stop sending traffic.

  Workaround: Use the **shut** and **no shut** commands on the subinterface that is carrying the PVC.

  Alternate Workaround: Enable ATM traffic shaping.

- CSCdr02061

  On the output Versatile Interface Processor (VIP) interfaces of a Cisco 7500/RSP series that is running Cisco IOS Release 12.0 S, Multiprotocol Label Switching (MPLS) packets are not classified correctly for Distributed Weighted Random Early Detection (DWRED) and Distributed Weighted Fair Queueing (DWFQ). In this situation, all MPLS packets will be considered class 0 by these algorithms regardless of the actual value of their MPLS experimental field values. There is no workaround.

- CSCdr02641

  A TI1575 ATM driver might reload with a bus error due to double freeing buffers. There is no workaround.

- CSCdr06072

  Multicast forwarding might stop for a specific group on the outgoing interface for a given multicast client if the client is pruned after leaving the group and later joins the group again. This condition occurs only in Protocol Independent Multicast (PIM) dense mode; PIM sparse mode is not affected.

  Workaround: Clear the multicast route for the group for that client by entering the **clear ip mroute** {*group*} command.

- CSCdr07280

  Snmpwalk on a Cisco 7500/RSP series router with an ATM interface might cause a CPUHOG situation and affect router performance. There is no workaround.

- CSCdr23302

  When you use Cisco Express Forwarding (CEF), generic routing encapsulation (GRE) tunnels, and tunnel checksums, the packet loss rate is abnormally high.

  Workaround: Disable tunnel checksums or disable CEF on the tunnel interface.

- CSCdr28435

  If you modify an interface maximum transmission unit (MTU), the saved MTU change is not read properly from the NVRAM configuration file upon reload. In a large Frame Relay environment, all Frame Relay links will be in a down state until a manual reconfiguration is done. There is no workaround.

- CSCdr29259

  Interface counters will give incorrect values for tunnels on a serial interface when Cisco Express Forwarding (CEF) and IP Security (IPSec) are in use. There is no workaround.

- CSCdr34877

  A memory leak might occur on a Route Switch Processor (RSP) when it is used with Versatile Interface Processors (VIPs) while running Open Shortest Path First (OSPF). The problem results due to repetitive reloading and downloading of VIP linecards that are disabling Cisco Express Forwarding (CEF) due to a lack of memory.

  Use the **show processes memory** [*inc OSPF R*] EXEC command and the **show memory summary** [*inc OSPF R*] EXEC command on the RSP to determine if increasingly large amounts of memory are being held by the OSPF process. Use the **show cef linecard** EXEC command to determine the number of reloads that a VIP has encountered.

  Workaround: Ensure that the VIPs have sufficient memory for their configuration and environment, such that CEF is not disabled on the VIP.

- CSCdr35715

  Under certain circumstances, a Cisco router might reload when crypto is enabled on a Fiber Distributed Data Interface (FDDI). There is no workaround.

- CSCdr40080

  A Cisco 12000 series Gigabit Switch Router might reload with a bus error at PC 0x600D3ED4, address 0x1B2DC330. There is no workaround.

- CSCdr44028

  If access lists with more than 1000 lines are used on a Cisco router that has compiled access control lists (ACLs) enabled, changes or additions to the ACLs might cause the router to exhibit a message similar to the following:

  ```
  SLOT 0:%SYS-3-CPUHOG: Task ran for 2928 msec (35/5),
  Process = TurboACL, PC = 4009274C
  -Traceback= 40092754 401AFED4 401AFB18 401B1474 401B2E60 401B2ED8 401B2FEC 40082128
  40082114
  ```

  In some situations, this condition might cause a failure with process keepalive messages that results in an undesired line protocol down state. There is no workaround.

- CSCdr46190

  When attaching a service policy in combination with Multiprotocol Label Switching (MPLS), the service policy will not take effect until the configuration is saved and the router is reloaded. There is no workaround.

- CSCdr48014

  Open Shortest Path First (OSPF) updates might be corrupted on a Cisco 7500 series router using Multiprotocol Label Switching (MPLS) switching with Cisco Express Forwarding (CEF) output features enabled (including "service policy output"). IP routes are temporarily deleted from the IP routing table and a loss of connectivity might occur.

  Workaround: Configure the **ip cef** global configuration command. Then, execute the **copy running start** command, and reload.

  Alternative workaround: Enter the **memory cache-policy io uncached** command. However, entering this command might sacrifice packet switching performance.

- CSCdr49601

  A Gigabit Ethernet Interface Processor (GEIP) on a Cisco 7500 series router might experience receiving problems that cause the router to pause indefinitely.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the gigabit interface. If the problem persists, perform a microcode reload on the router to disrupt all interfaces.

- CSCdr51003

  Enabling or disabling output access control lists (ACLs) might cause a 3-port Gigabit Ethernet (GE) card in the router to restart. There is no workaround.

- CSCdr52838

  PA-MC-8T1 reported firmware hung and then crashed the router. There is no workaround.

- CSCdr52879

  A Cisco 12000 series Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(11)S might exhibit error messages similar to the following:

  ```
  SLOT 6:00:21:00: %LC-3-MACSTR: Adj/midb (MDS 224.101.1.1) incorrect macstring:
  length=12, macstr word=0x00180100
  -Traceback= 402AE924 402F9BD8 402F5A5C 402F7D84 402F7E70 402F7638 4009B974 4009B960
  ```

  In this situation, IP Multicast on ATM cards might not function properly. This condition only affects ATM cards. There is no workaround.

- CSCdr52927

  A channelized OC-12 STS-3c/STS-1 line card might not properly create internal loops. In this situation, no tests will run through the looped OC-3. There is no workaround.

- CSCdr53138

  A Gigabit Ethernet interface might remain in an up/up state with no cable attached when running Cisco IOS Release 12.1(2). This condition can cause problems when running Hot Standby Router Protocol (HSRP) with the Gigabit Ethernet interface and might also cause routing black holes. There is no workaround.

  A Gigabit Ethernet interface might remain in an up/up state with no cable attached when running Cisco IOS Release 12.1(2). This condition can cause problems when running Hot Standby Routing Protocol (HSRP). The result is that if the active router fails, the backup router will take over; however, any traffic destined for the local segment from the original active router will be dropped. There is no workaround.

- CSCdr57725

  On a Cisco 12000 series Gigabit Switch Router (GSR), the performance card might double-count software-switched input packets. The packet count for hardware-switched packets is not affected.

  Workaround: Do not configure Gigabit Ethernet static routes to another adjacent Gigabit Ethernet interface.

- CSCdr64798

  In certain configurations, the ATM permanent virtual connection (PVC) service policy might not function properly after the router has reloaded. In this situation, there are no feature counters in the **show policy interface** command output.

  Workaround: Remove and then reattach the service policy after the router is reloaded.

- CSCdr65982

  If the **fair-queue** interface configuration command is entered more than once within the same class in which weighted fair queueing is already enabled on that same interface, the router might reload. There is no workaround.

- CSCdr73378

  When the packet switch ASIC (PSA) access list (ACL) feature is enabled by entering the **access-list hardware** {**psa**} global configuration command and the feature was previously disabled with the **no access-list hardware** {**psa**} command, output ACLs that should be processed by the PSA might be processed on the line card CPU.

  Workaround: Avoid toggling the state of the **access-list hardware** {**psa**} command. This situation will not occur if the command is in the startup configuration and is not toggled.

- CSCdr73473

  Removing and attaching a service policy under a traffic load might cause spurious memory access errors and high CPU utilization on the Versatile Interface Processor (VIP). This spurious access occurs at hqf_get_policymap().

  Workaround: Stop background traffic before making configuration changes.

- CSCdr74025

  The spatial reuse protocol (SRP) line card on a Cisco 12000 series Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(11.5)S might reload unexpectedly upon start-up. There is no workaround.

- CSCdr75209

  When Frame Relay fragmentation is configured after attaching a traffic-shaping service policy to a large number of permanent virtual connections (PVCs), the service policy might not function properly. Since Frame Relay fragmentation appears after “service-policy” in the configuration order, there is a chance that this situation will occur after a system reload. The specific policy that fails is:

  ```
  policy-map fr-pvc
  class class-default
  shape average <cir>
  service-policy llq-policy
  ```

  Workaround: Configure **service-policy** after FR fragmentation, or add **queue-limit** to the traffic shaping policy as follows:

  ```
  policy-map fr-pvc
  class class-default
  shape average <cir>
  queue-limit <n>
  service-policy llq-policy
  ```

- CSCdr75997

  CSCdm94333, which was integrated in Cisco IOS Release 12.0(9.6)S, introduced a new version of the automatic protection switching (APS) protect group protocol that required both working and protect routers to be upgraded simultaneously. The fix for CSCdr75997 relaxes this restriction by supporting interoperability between systems that are running different versions of the APS protocol so that working and protect can be upgraded independently.

- CSCdr80820

  A Cisco 12000 series Gigabit Switch Router (GSR) that is configured for distributed IP multicast might exhibit the following error messages:

  ```
  SLOT 8:03:43:10: %ALIGN-3-SPURIOUS: Spurious memory access made at 0x402EB90C reading
  0x0
  SLOT 8:03:43:10: %ALIGN-3-TRACE: -Traceback= 402EB90C 402E779C 402E9AC4 402E9BA8
  402E9388 4009B02C 4009B018 00000000
  SLOT 8:03:43:10: %ALIGN-3-TRACE: -Traceback= 402EB910 402E779C 402E9AC4 402E9BA8
  402E9388 4009B02C 4009B018 00000000
  ```

  There is no workaround.

- CSCdr80686

  When a rate-limiting feature (for example, committed access rate (CAR)) or a QoS feature (for example, access-control list (ACL)) is enabled on an interface of an Engine 0 or Engine 1 line card on a Cisco 12000 series Gigabit Switch Router (GSR), the receive (RX) byte and packet counters for that inteface shows the net number of byte and packets that have been admitted to the interface. In this situation, packets that are dropped at the interface because of CAR or ACL are excluded from the RX byte and packet counters. There is no workaround.

- CSCdr81657

  When there is no feature enabled on a Route Switch Processor (RSP), a Cisco Express Forwarding (CEF) switched packet (as opposed to a distributed CEF packet) will cause spurious memory access in atm_set_cli_wrapper(). There is no workaround.

- CSCdr81857

  If a QoS service-policy is configured on a channelized interface on a PA-MC-T/E1 or PA-MC-T/E3 port adapter, entering the **microcode reload** global configuration command under heavy traffic might result in a failure to forward packets for the interface.

  Workaround: Remove the service-policy before entering the **microcode reload** command, and then reapply the policy.

- CSCdr83067

  If the **clear counters** EXEC command is entered from a Secure Shell (SSH) connection on a router with E1/T1 controllers, a "SYS-3-CPUHOG" error message might be exhibited. This condition occurs when the **clear counters** command fails on more than one E1/T1 controller with a "POT1E1-3-MBOXSEND" error.

  Workaround: Clear each E1/T1 controller individually.

- CSCdr83141

  Under certain circumstances, configuration on an ATM permanent virtual connection (PVC) might fail with the following erro message:

  ```
  ATM hardware failed cannot update vc
  ```

  If Operation, Administration, and Maintenance (OAM) is also configured, the router might reload after the error.

  Workaround: Do not enter the **show policy interface** global configuration command.

- CSCdr91303

  When attaching and removing a QoS service-policy under a heavy traffic load on a channelized interface on a MC-T/E1 or MC-T/E3 port adapter, packets might stop forwarding out of the interface.

  Workaround: Enter the **microcode reload** global configuration command.

- CSCdr91482

  The Cisco 12000 series Gigabit Switch Router (GSR) will incorrectly increment the input drops counter because of an accounting issue. This action might not correctly reflect packets dropped because of congestion. This sitution might be seen on all GSR interfaces, but has no effect on service or functionality of the interfaces. There is no workaround.

- CSCdr95090

  When a policy map is attached to an interface on a Cisco 7200 series router, the router experiences spurious memory access at the function hqf_get_policymap(). There is no workaround.

Wide-Area Networking

- CSCdr43764

  Extracting 64-bit Simple Network Management Protocol (SNMP) counters for the Frame Relay interface on a Packet-over-SONET (POS) interface might not work. This condition applies to both the relevant IF-MIB counters and the Cisco-specific 2 x 32-bit counters in CISCO-C12000-IF-HC-COUNTERS-MIB and relates only to the Frame Relay 64-pit permanent virtual connection (PVC) counts when a Frame Relay encapsulated interface is added to a POS interface. The main POS interface counters are not affected and continue to function properly.

  Workaround: Upgrade to an image that contains this patch.

Resolved Caveats—Cisco IOS Release 12.0(11)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(11)S. This section describes only severity 1 and 2 caveats.

Interfaces and Bridging

- CSCdp08975

  A Cisco 7200 router that is configured for RFC1577 and is not acting as an Address Resolution Protocol (ARP) server might experience a condition in which the status of ATM VCs might change in spite of the traffic flowing on them. This condition occurs if RFC1577 is configured on the main interface.

  Workaround: Configure RFC1577 on a subinterface.

- CSCdp71620

  A Cisco Packet OC-3 Interface Processor (POSIP) might reload with a bus error. There is no workaround.

IP Routing Protocols

- CSCdp95210

  Under rare circumstances, a link-state advertisement (LSA) on a neighboring router might get stuck in MAXAGE state and not be deleted. In this situation, the LSA cannot be originated again on this router, and the route might become unavailable or cause packets to take another route that is less than optimal. This situation has been seen to occur when an OSPF neighbor ran out of memory and OSPF tables are corrrupted.

  Workaround: Restart the OSPF process by entering the **clear ip ospf proc** command.

- CSCdr07966

  On a Cisco 7500 series router, many Virtual Private Networks (VPNs) configured in combination with a large number of channelized interfaces might result in a FIBDISABLE message.

  The FIBDISABLE message indicates that the Route Processor (RP) has not received a Forwarding Information Base (FIB) “keepalive”message from the line card in the expected amount of time. When this situation occurs, the RP acts as if the interprocess communication (IPC) mechanism had malfunctioned and disables Cisco Express Forwarding (CEF) on that line card.

  Workaround: Disable distributed switching.

- CSCdr27994

  When tearing down a link-state packet (LSP) reservation, Resource Reservation Protocol (RSVP) sends the upstream neighbor a ResvTear message that contains a RESV_CONFIRM object. RSVP maintains the reservation and continues to send this message periodically until the upstream neighbor responds with a ResvTearConf message or the reservation times out.

  If the downstream neighbor continues to send Resv refreshes for the LSP, the reservation will never time out. In this situation, if the upstream neighbor never sends a ResvTearConf message, the reservation remains in this state indefinitely. The ResvTearConf mechanism is no longer defined in the RSVP-TE IETF draft and is no longer used by some non-IOS implementations. There is no workaround.

- CSCdr35856

  If you enter the **show ip mds summary** EXEC command or the **show ip mds forwarding** EXEC command at the Versatile Inter face Processor/line card (VIP/LC) console, then a counter to track the number of multicast routes might be incorrectly decremented and underflow to a huge number. The VIP/LC console might display a syslog message similar to the following:

  ```
  %MDS-4-ROUTELIMIT: 4294967237 routes exceeded multicast route-limit of 2147483647
  ```

  If this situation occurs, no additional multicast routes can be created and the router must be restarted.

  Workaround: Do not use the **show ip mds summary** EXEC command or the **show ip mds forwarding** EXEC command at the VIP/LC console.

- CSCdr45483

  A Cisco router with multicast configured might reload with a bus error if there are severe unicast route updates. There is no workaround.

ISO CLNS

- CSCdr09770

  Configuring a tunnel bandwidth requirement change to a Multiprotocol Label Switching/traffic engineering (MPLS/TE) tunnel might cause Intermediate System-to-Intermediate System (IS-IS) routes that are accessible through that tunnel interface and their corresponding Cisco Express Forwarding (CEF) entries to be unnecessarily reinstalled when subsequent shortest path calculations are done.

  Workaround: If MPLS/TE announces new tunnel information to IS-IS routes after the bandwidth change has taken effect, this spurious RIB updates behavior can be cleared. The following are a few actions that can clear this behavior:

  – Configuring an MPLS/TE tunnel metric

  – Adding or removing MPLS/TE tunnels to the same tail-end as the tunnel that changed bandwidth. This can include both the current MPLS/TE tunnel and additional tunnels to the same tail-end.

- CSCdr21706

  A Cisco router that is running Cisco IOS Release 12.0(3.5)S or later releases might experience a reload with both Border Gateway Protocol (BGP) and Intermediate System-to-Intermediate System (IS-IS) routing running and a configuration setting the BGP administrative distance to 115. In this situation, the following traceback immediately precedes the reload (<> indicates a variable value):

  ```
  %CLNS-1-BKUPERR: ISIS: No NDB back pointer in 0x<>, ndb_next 0x0, ndb_prev 0x0, lsp_next
  0x0, lsp_prev 0x0, metric 0x0, index 0, 0x0
  ```

  Workaround: Configure a BGP administrative distance different from 115.

Miscellaneous

- CSCdm69594

  The interface delay metric is set incorrectly for port channel interfaces where one or more Gigabit Ethernet interfaces are grouped into a channel. The delay for a single Gigabit Ethernet interface is 10 microseconds. The delay for a port channel made up of one or more Gigabit Ethernets is 100 microseconds. The incorrect setting might seriously impact routing protocols that use interface

delay as part of the metric (for example, Enhanced Interior Gateway Routing Protocol (EIGRP)), and might cause the routing protocol to take a route through a single interface over a route through a port channel.

Workaround: Manually configure an appropriate delay under the port channel interface by entering the **delay** *tens of microseconds* interface configuration command.

- CSCdm78020

  Performance OC-48 POS and QOC-12 POS line cards might not fragment Multiprotocol Label Switching (MPLS) packets or send Internet Control Message Protocol (ICMP) messages if the DF bit is set in the header of the IP Payload of MPLS packets requiring fragmentation.

  Workaround: Change the maximum transmission unit (MTU) on the interface to be less than or equal to the MTU on the next hop.

- CSCdm94154

  A Cisco 7200 series router that is configured with a T1 multichannel T1 card might not show any errors while a remote Cisco 7000 series router shows cyclic redundancy check (CRC) errors, input frame errors, or overrun errors. Errors occur, but the counter remains at zero. There is no workaround.

- CSCdp23658

  Tunnels that are configured for multicast routing and multicast distributed switching might cause a Cisco 12000 series Gigabit Switch Router (GSR) to reload with a bus error.

  Workaround: Do not configure the tunnel for multicast routing by entering the **ip pim** {**foo-mode**} interface configuration command. If you must configure the tunnel interface for multicast routing, enter the **no ip mroute-cache** interface configuration command.

- CSCdp48087

  A Cisco 12000 series Gigabit Switch Router (GSR) with dual gigabit route processors (GRPs) might exhibit the following error message if the primary GRP reloads and the secondary GRP takes over:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 2: No window > message, LC to RP IPC is
  non-operational
  ```

  This error message will disable the line card, and the line card must be reloaded manually before it comes back online. There is no workaround.

- CSCdp51945

  On a Cisco 7500 series RSP router, a Simple Network Managment Protocol (SNMP) get query of cieNumberOfConnections (.1.3.6.1.4.1.9.9.52.1.3.1.0) results in spurious access. This condition can also lead to a memory leak in the IP SNMP process. There is no workaround.

- CSCdp56613

  When fast-switching an IP frame that is fewer than 46 bytes in length to an ATM interface, the router always sets the length in the ATM adaption layer 5 (AAL5) header to 54 bytes even though the length should be equal to the IP frame length plus the length of the AAL5 header, which is 8 bytes. There is no workaround.

- CSCdp58964

  A Cisco router that is running Cisco IOS Release 12.0(7)S or Cisco IOS Release 12.0(8)S will disable Cisco Express Forwarding (CEF) with a FIB-3-NOMEM failure even though there appears to be plenty of memory. There is no workaround.

- CSCdp78089

  When the environmental values for voltage get corrupted and a Cisco 12008 Gigabit Switch Router (GSR) has all slots at the critical warning level, entering the **show run** command causes the router to shut down. This condition is more likely to occur after a router has been up and running for several weeks or more. There is no workaround.

- CSCdp83870

  Proper Multiprotocol Label Switching (MPLS) fragmentation is not done for some packet sizes on a Cisco 12000 series gigabit switch router (GSR) when the output interface is Fast Ethernet (FE) or Gigabit Ethernet (GigE). There is no workaround.

- CSCdp90558

  When the **atm pvp** interface configuration command is entered on a Cisco 12000 Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(8.5)S or higher releases, two F4 Operation, Administration, and Maintenance (OAM) virtual circuits (VCs) are automatically created. There is no workaround.

- CSCdr02906

  A Cisco router might experience spurious memory access in function lc_qos_supported() when the **show running-config** command or the **show startup-config** command is entered and exhibit a traceback similar to the following:

  ```
  Reading rsp-jsv-mz.121-1.0.2.T.symbols rsp-jsv-mz.121-1.0.2.T.symbols read in Enter hex
  value: 0x603BD8E4 0x61266454 0x602C4E3C 0x602CD2C4 0x602CD45C 0x60278 88C 0x6025EF40
  0x6025F2A8 0x603BD8E4:lc_qos_supported(0x603bd89c)+0x48
  0x61266454:distributed_feature_enable(0x6126632c)+0x128
  0x602C4E3C:prioritygroup_command(0x602c4df8)+0x44
  0x602CD2C4:eol_action(0x602cd240)+0x84 0x602CD45C:eols_action(0x602cd440)+0x1c
  0x6027888C:parse_token(0x6027854c)+0x340
  0x6025EF40:nv_current_common(0x6025ede8)+0x158
  0x6025F2A8:nv_current_to_new_buffer(0x6025f1d8)+0xd0 Enter hex value:
  ```

  This situation will occur if one or more Fast Ethernet channels are configured by entering the **interface port-channel** command. There is no workaround.

- CSCdr04630

  Packets that are destined to IP prefixes using recursive routes over Multiprotocol Label Switching/traffic engineering (MPLS/TE) tunnels might be dropped by OC-48 Packet over SONET (POS) and QOC-12 POS line cards for the Cisco 12000 series gigabit switch router (GSR) at the head end of the tunnnel. There is no workaround.

- CSCdr08160

  Under heavy traffic on the outbound side of a Spatial Reuse Protocol (SRP) port adapter, packets will get queued on holdq if the TX ring is full. These packets will be accounted as process switched instead of route-cache switched. There is no workaround.

- CSCdr15506

  When 802.1Q is configured on a Cisco 12000 series gigabit switch router (GSR) Gigabit Ethernet (GigE) line card, the following error message might be displayed:

  ```
  %LC-3-BMACMDLOST: ToFab BMA has lost a command
  ```

  There is no workaround.

- CSCdr16178

  When an access control list (ACL) is applied to an interface and the ACL has destination prefixes in it that are more specific than a route that is learned recursively, packets that match the ACL entry with that destination prefix will not be routed correctly in the “permit” case.

  For example, if there are the following static routes:

  ```
  ip route 70.0.0.0 255.0.0.0 pos 1/0 ip route 80.0.0.0 255.0.0.0 70.1.1.1 ip route
  90.0.0.0 255.0.0.0 80.1.1.1
  ```

  and an ACL is applied with the following rule:

  ```
  access-list 101 permit ip any host 90.1.1.1
  ```

  the route to 90.0.0.0/8 is recursive and 90.1.1.1 is more specific than this route; packets destined to 90.1.1.1 will not get routed to their destination.

  This situation will only occur if the route is learned or applied after the ACL is applied to the interface. If the ACL is applied after the routes are learned, this situation does not occur.

  Workaround: Remove and reapply the ACL after a recursive route is learned or applied.

- CSCdr17190

  If Resource Reservation Protocol (RSVP) receives Path messages for the same label-switched path (LSP) session on two different interfaces, RSVP may enter a state where it sends Resv messages alternately on those interfaces and where only the Resv messages sent on one of the interfaces contains a label for the LSP.

  In the event a single device is receiving the alternating Resv messages, which could happen if the sending and receiving devices are connected by parallel links, the receiving device will update its forwarding table entry for the LSP on receipt of each Resv.

  Receipt of the Resv with no label will cause the receiving node to install a "label pop" entry. Packets arriving at the receiving node on the LSP in question will have their top label popped incorrectly.

  Workaround: Shut down the LSP tunnel interface at the LSP head device and wait for the RSVP state for the LSP to time out of the network.

- CSCdr19089

  When deleting a port-channel subinterface on a Cisco 7500/RSP series router that is running Cisco IOS Release 12.0(10)S, the entire interface (both main and subinterfaces) is deleted rather than just the selected interface. There is no workaround.

- CSCdr19213

  If packet switch ASIC (PSA) access control lists (ACLs) are applied on a Cisco 12000 series gigabit switch router (GSR), packets that ingress on a PSA-enabled card and egress on a non-PSA card (Engine 0 or Engine 1) will not appear in the outbound **show interface** counters even though these packets are forwarded properly.

  This situation only affects the outbound packet accounting (shown by the outbound packet rate counter) and the outbound packet counter. Input byte and packet rate counters are not effected. Packets that egress the router on a PSA (Engine 2) card are counted correctly. There is no workaround.

- CSCdr21181

  When Cisco Express Forwarding (CEF) is enabled on a Gigabit Route Processor (GRP) E0 interface on a Cisco 12000 series gigabit switch router (GSR) and the router is reloaded, the **ip route-cache cef** interface configuration command is lost after the reload. The default behavior was changed for this interface as of Cisco IOS Release 12.0(8.6)S by CSCdm01200. This change

disables **ip route-cache cef** by default, and it has changed the forwarding behavior as well. When the command is disabled, packets will not be routed through the GSR if they come in on this interface.

Workaround: Upgrading past CSCdr21181 will allow you to configure the **ip route-cache cef** command, and the command will survive all consecutive reloads if you save it to NVRAM.

- CSCdr23697

  When distributed Cisco Express Forwarding (dCEF) is enabled on spatial reuse protocol (SRP) IP doing sam- interface routing, on a Cisco 7500 router that is running Cisco IOS Release 12.0(8)S, traffic will not be sent out the SRP interface.

  Workaround: Change from first-in first-out (FIFO) to priority queueing (PQ).

- CSCdr24628

  An OC-48E/POS line card might restart with a software forced crash. This condition occurs due to Multicast, and the following error messages are seen in the log:

  ```
  LC-3-TBMMCAST: tbmm_tbl_remove_ent_port: invalid hw_mdb/midb
  LC-3-TBMMCAST: tbmm_remove_ent_port: port not set
  ```

  Workaround: Remove Multicast from the configuration.

- CSCdr24842

  If input MAC accounting is configured on an interface, misaligned read accesses might be encountered on the Cisco 7500 series route switch processor (RSP). The **show alignment** command should be entered to determine if misaligned accesses are occurring.

  Workaround: Disable input MAC accounting on the interface.

- CSCdr25771

  A Cisco 12000 series gigabit switch router (GSR) spatial reuse protocol (SRP) line card might reload when a node on the SRP ring contains a MAC address that ends with the value 0800 or 8847.

  Workaround: Change the value of the last two bytes of the MAC address.

- CSCdr27954

  Under rare circumstances, the processing of re-resolving a previously known Address Resolution Protocol (ARP) entry might cause errors in the packet switch ASIC (PSA) access control list (ACL) processing, which leads to the incorrect blocking of packets into a PSA-enabled card. This condition occurs when output ACLs are configured on the Gigabit Ethernet (GE) interface and PSA ACLs are in the inbound direction on the PSA card.

  Workaround: Remove either the input or the output ACL and reapply it, which forces a rebuild of the PSA data structures and clears the problem.

- CSCdr28169

  A Cisco router that is running Cisco IOS Release 12.0 S might reload or experience spurious memory access if **set atm-clp** is configured in an attached policy map and then removed while the policy map is still attached. This situation might also occur if a policy map that is configured with **set atm-clp** is attached and detached from an interface. There is no workaround.

- CSCdr29540

  A Cisco 12000 series gigabit switch router (GSR) with dual gigabit route processors (GRPs) that is running Cisco IOS Release 12.0(9.6)S or 12.0(10)S might experience difficulties with the serial console after a failover. Both GRPs in a GSR dual GRP setup might have individual serial console connections (for example, there is no “Y” cable). If you use the serial console that is attached to the secondary GRP then this is automatically connected through to a vty on the primary GRP. If there is a failover while the secondary console is in use, the console is not released from the vty

session. The console is inoperative until the old primary GRP has rebooted, at which time the vty connection is reestablished. The effect is similar to an attach session being started. A symptom of this situation is that the prompt has the form “GRP-Slot#”.

Workaround: After a failover, type **exit** to leave the unwanted session with the other GRP. This action should return the console to a normal state. This action will only work if the failed GRP has rebooted to become the secondary GRP. If the failed GRP does not reboot, the serial console will effectively remain locked. To recover from this, use Telnet to log in to the router and enter the **clear line** *0* command. To prevent this situation from occurring again, avoid any use of the console on the secondary GRP.

- CSCdr29594

  A Cisco 7500 series route switch processor (RSP) with ATM interfaces might pause indefinitely under the the following conditions:

  – A microcode reload

  – A change in the maximum transmission unit (MTU)

  – A change in the encapsulation

  Workaround: A possible workaround is to put all the ATM interfaces in admin down state during the above operations.

- CSCdr33450

  DML-PPP does not function properly on a VIP4-80 Versatile Interface Processor. The VIP4 will reload, and the controller will be in a shutdown state. There is no workaround.

- CSCdr34945

  The Cisco 12000 series gigabit switch router (GSR) is unable to switch packets from an ingress line card interface to the section data communication channel (SDCC) that is communicating with a Cisco Optical Regenerator. In this situation, the Cisco Optical Regenerator might display the following error message:

  ```
  Illegal HDLC serial type code 60, PC=0x801410C4
  Illegal HDLC serial type code 60, PC=0x801410C4
  ```

  The Cisco Optical Regenerator can only be managed from the E0 interface of the gigabit switch router (GSR). There is no workaround.

- CSCdr40080

  A Cisco 12000 series gigabit switch router might reload with a bus error at PC 0x600D3ED4, address 0x1B2DC330. There is no workaround.

- CSCdr40808

  On Performance OC-48, QOC-12, and 16-port OC-3 line cards, the Time To Live (TTL) value is not propagated correctly on receipt of a Multiprotocol Label Switching (MPLS) packet with a label stack of more than one label when performing a label swap or a label pop operation. There is no workaround.

- CSCdr42456

  If you attempt to set a class queue limit by entering the **fair-queue** [**qos-group**|**tos**] *value* **limit** *value* command, the **limit** command does not function properly, and the queue limit will always remain at the default value. There is no workaround.

- CSCdr44028

  If access lists with more than 1000 lines are used on a Cisco router that has compiled access control lists (ACLs) enabled, changes or additions to the ACLs might cause the router to exhibit a message similar to the following:

  ```
  SLOT 0:%SYS-3-CPUHOG: Task ran for 2928 msec (35/5), Process = TurboACL, PC = 4009274C
  -Traceback= 40092754 401AFED4 401AFB18 401B1474 401B2E60 401B2ED8 401B2FEC 40082128
  40082114
  ```

  In some situations, this condition might cause a failure with process keepalive messages that results in an undesired line protocol down state. There is no workaround.

- CSCdr46240

  If the **crypto key generate rsa** global configuration command has been included in the startup-config file, the router may reload during key generation when the startup-config is processed.

  Workaround: Exclude the **crypto key generate rsa** global configuration command from the startup-config file, and manually configure the RSA key-pair from the console session.

- CSCdr47488

  Netflow does not function properly for Engine 0-based cards on a Cisco 12000 series gigabit switch router (GSR) that is running Cisco IOS Release 12.0(10.1)S to 12.0(10.5)S.

  Workaround: Use sampled netflow.

- CSCdr48846

  If a hardware error occurs on a Performance OC-48 line card where an application specific integrated circuit (ASIC) on the line card must be reset to recover, the line card might experience problems forwarding Multiprotocol Link Switching (MPLS) traffic. The line card will require a microcode reload to fully recover. There is no workaround.

- CSCdr49629

  When an output access control list (ACL) is used, the line card might produce some tracebacks while running Cisco IOS Release 12.0(10.1)S to 12.0(10.5)S. This message is harmless, and the only side-effect of this condition is that the log message will be printed. There is no workaround.

Wide-Area Networking

- CSCdr43764

  Extracting 64-bit Simple Network Management Protocol (SNMP) counters for the Frame Relay subinterface on a Packet-over-SONET (POS) interface might not work. This condition applies to both the relevant IF-MIB counters and the Cisco-specific 2 x 32-bit counters in CISCO-C12000-IF-HC-COUNTERS-MIB and relates only to the Frame Relay 64-bit PVC counts when a Frame Relay encapsulated interface is added to a POS interface. The main POS encapsulated subinterface counters are not effected and continue to function properly.

  Workaround: If the 32-bit equivalent SNMP counters from the IF-MIB are retrieved with a fast enough polling cycle that the counters can be guaranteed not to wrap between polls, the 64-bit SNMP counters are not necessary.

Resolved Caveats—Cisco IOS Release 12.0(10)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(10)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdp45379

  A Cisco 7200 series router with an NPE-300 network processing engine installed might not boot up when certain Cisco IOS Release 12.0(5)XE3 subset images are installed. The router will pause indefinitely in the early stage of booting up, and a power cycle is required to resume. For systems set for auto boot, you will need to enter the **break** command to abort the boot process and break out to the ROM monitor before the 12.0(5)XE3 image is launched for execution. You will then need to either modify the software configuration register to revert to a manual boot of some other known good image, or you will need to switch the PCMCIA flash card with a known good image in case the system is set for a default image boot from the slot0: PCMCIA card. There is no workaround.

Interfaces and Bridging

- CSCdm06860

  Cisco IOS Release 11.1(24)CC might return a wrong value for MIB object cardType for PA-POSSW-MM/SM port adapters due to the Simple Network Management Protocol (SNMP) agent in the Cisco IOS Release 11.1(24)CC. Values for PA-POSSW 401 are returned instead of values for PA-POSSW 564 and PA-POSSW 564. There is no workaround.

- CSCdm11933

  CT3/CE3 port adapters on a Cisco 7200 series router might drop TX packets under bursts of heavy traffic instead of putting them in a hold queue if the number of outstanding transmit packets temporarily exceeds the number specified by the TX limit. There is no workaround.

- CSCdp60859

  When a channel on a CT3/CE3 port adapter is continually overstressed by traffic, other nonstressed channels might experience some transmit packet drops. There is no workaround.

- CSCdp99579

  Configuring an Async interface in any Cisco 7500 series Route Switch Processor (RSP) will prevent the proper parsing of interface name for CT3/CE3 port adapters.

  Workaround: Deconfigure any Async interface, and then write the configuration to NVRAM and reload the router. Or, you can move the VIP from slot 0 to another slot.

- CSCdr00681

  A Channelized T3 Interface Processor (CT3IP) driver on a Cisco 7500 series router might leak particles from the receiving side, which results in the CT3IP seeing all serial interfaces as flapping after a few hours. This situation can be observed by checking input errors in the **show interface** output. There is no workaround.

IP Routing Protocols

- CSCdp18787

  A Cisco router that has tag switching enabled and is running Cisco IOS Release 12.0(5)T might reload if a tag advertisement appears in a certain time window when a related routing update takes place. An ATM interface transition might cause this condition. There is no workaround.

- CSCdp43545

  Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels might bounce under certain conditions if there is a very heavy traffic load on a Gigabit Switch Router (GSR) line card. This condition has been observed when a routing loop is present and the card is generating Internet Control Message Protocol (ICMP) "TTL expired" messages, and when the card is used as the data sink for ICMP ECHO requests from a traffic generator. There is no workaround.

- CSCdp72309

  A Cisco router that is running Cisco IOS Release 12.0(8)S might reload with a bus error at ospf_default_networkupdate after links flap or the **clear ip bgp** {*****} EXEC command is entered. There is no workaround.

- CSCdp85688

  When a Multicast Routing Monitor (MRM) Test Sender is instructed by an MRM Manager to send test packets out of all interfaces that are configured for multicast routing, which is the default option, the MRM might experience a leak in the small buffers.

  Workaround: Configure the MRM Manager with the **senders** {**access-list-number** | **access-list-name**} [*target-only*] command.

Miscellaneous

- CSCdm64005

  A PA-T3 port adapter might exhibit a timing problem resulting in dropped packets. There is no workaround.

- CSCdm75813

  Writing to an AT Attachment (ATA) device might cause the device to become unusable and result in an "ATA_Status time out waiting for 1" error message.

  Workaround: Reload the Cisco IOS software.

- CSCdm94333

  In APS configurations in which working and protect interfaces are in different routers, if a direct link between the two routers fails and is replaced by an indirect IP route, then the router containing the working interface will have no IP address for the router that is housing the protect interface. The resulting communications failure might result in both interfaces being deselected or both interfaces being selected. There is no workaround.

- CSCdp16749

  When Turbo Access Control Lists (Turbo ACLs) are enabled when the **access-list compiled** command is entered, reloading or reinstalling multiple access lists might cause a reload or an alignment error. This condition is most likely to occur on Cisco 12000 series Gigabit Switch Router (GSR) line cards, and usually occurs when many access list lines are being copied into the configuration.

  Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

- CSCdp34046

  If an output rate limit is configured on a non-Versatile Interface Processor (VIP) interface (for example, AIP or FIP) on a Cisco 7500 series Route Switch Processor (RSP) with Cisco Express Forwarding (CEF) enabled, packets cannot be switched out of that interface.

  Workaround: Disable CEF.

- CSCdp46780

  After the primary clock scheduler card (CSC) has been removed, a Cisco OC-48/STM-16 Packet-over-SONET/SDH line card might not recover from being switched to the secondary CSC card and report error messages.

  Workaround: Reload the line card.

- CSCdp54069

  A Cisco PA-2T3 port adapter might show increasing overruns in the **show interface** command output display when one of the two ports is in a DOWN state.

  Workaround: Configure the **serial restart** *0* command on the DOWN interface, or put the DOWN port in ADMIN SHUT state.

- CSCdp54813

  A Cisco 7500 series router will often reload when switching onto an IP tunnel if sending to the tunnel destination involves Multiprotocol Label Switching (MPLS) label imposition. There is no workaround.

- CSCdp61411

  A Cisco 7200 series router might receive a large number of alignment errors in the Cisco Express Forwarding (CEF) FastPath, which causes severe performance degradation.

  Workaround: Disable CEF by entering the **no ip cef** global configuration command.

- CSCdp64140

  Two Cisco 12000 series Gigabit Switch Routers (GSRs) that are connected by a Gigabit Ethernet connection might exhibit “GRP-4-CORRUPT” error messages when one of the routers is upgraded to Cisco IOS Release 12.0(8)S. There is no workaround.

- CSCdp71623

  Packets that have been padded by the previous hop that are received by a Versatile Interface Processor (VIP) Ethernet/Fast Ethernet/Gigabit Ethernet router might be dropped if those packets are supposed to be processed by the Route Processor rather than by the VIP.

  Workaround: Disable distributed Cisco Express Forwarding (dCEF) on the ingress interface.

- CSCdp72483

  If a Cisco 12012 or Cisco 12016 Gigabit Switch Router (GSR) that is running Cisco IOS Release 12.0(7)S or 12.0(8)S with dual gigabit route processors (GRPs) experiences a failover, full bandwidth line cards might not boot correctly, and the router will exhibit a “MBUS-3-INSUFF_BW” message. A microcode reload is needed to make the line cards function properly again. This condition is rare.

  Workaround: If you are upgrading a GSR with dual GRPs and full fabric line cards to Cisco IOS Release 12.0(7)S or 12.0(8)S, check that all line cards initialize correctly after a dual GRP failover. You can test this condition by entering the **redundancy force-failover** EXEC command. If the check fails, then you will need to use a different image.

- CSCdp74038

  On Gigabit Ethernet line cards, 802.1Q packets that are 512 bytes and larger might get dropped on input. There is no workaround.

- CSCdp74616

  On the Cisco OC-48c/STM-16c and Cisco QOC-12 line cards for the Cisco 12000 series Gigabit Switch Router (GSR), there is a timing problem during initialization that might cause the line cards to reload if Multiprotocol Label Switching (MPLS) packets are received before the initialization is complete. There is no workaround.

- CSCdp78781

  A memory leak in a Cisco 12000 series Gigabit Switch Router (GSR) line card in the Cisco Express Forwarding (CEF) line card statistics might not clear quickly and exhibit high memory utilization. In this situation, the router exhibits the following stack trace:

  ```
  glc1-lc-m.120-8.3.S.symbols read in Enter hex value: 400A0314 400A1DC0 4027D3EC
  40279794 4009AA6C 4009AA58 0x400A0314:report_malloc_failure(0x400a02d4)+0x40
  0x400A1DC0:malloc(0x400a1aa4)+0x31c
  0x4027D3EC:fib_collect_frpvc_rxstats(0x4027d3b4)+0x38
  0x40279794:fib_lc_stats_background(0x402796c0)+0xd4
  0x4009AA6C:r4k_process_dispatch(0x4009aa58)+0x14
  0x4009AA58:r4k_process_dispatch(0x4009aa58)+0x0
  ```

  Workaround: Limit the size of the access lists, or do not use access lists.

- CSCdp80282

  Packets that are sourced from a Cisco 7500 series router with Multiprotocol Label Switching (MPLS) enabled and exit the router through a T1 or Channelized T1 connection will not be sent correctly. Other traffic traversing the router is not affected. There is no workaround.

- CSCdp82125

  A Route Switch Processor (RSP)-based router with one or more Versatile Interface Processors (VIPs) that is running Cisco IOS Release 12.0 S (or any image with tag support) might experience a memory leak with Cisco Express Forwarding (CEF) and tag switching enabled and the **no ip route-cache distributed** command configured. This memory leak can be detected by repeatedly entering the **show process memory** | **include OSPF** command on the RSP console or vty.

  Workaround: Enable distributed CEF instead of CEF, or turn off tag switching.

- CSCdp88204

  If the **tx-ring-limit** command is entered on a Cisco 7500 series Route Switch Processor (RSP) that is running Cisco IOS Release 12.0 S, the router might experience a NULL pointer access, and the Versatile Interface Processor (VIP) might reload. This situation occurs during line flapping and when the router is being configured. There is no workaround.

- CSCdp89965

  Under rare circumstances, a tunnel might have a drop adjacency on the line card while simultaneously having a valid adjacency on the on the Route Processor (RP).

  Workaround: Enter the **clear cef linecard** command to download the correct information to the line card.

- CSCdp86111

  When Cisco Express Forwarding (CEF) is configured as part of a large configuration (typically with access lists), following boot traffic that is directly addressed to the interfaces of a router might not be received. This condition can be observed on enabled interfaces where IP interfaces appear to be up, but the CEF interfaces are down.

  Workaround: Perform one of the following steps.

  – Boot without CEF enabled.

  – Disable and then re-enable CEF.

  – Enter the **no shutdown** command on each of the interfaces that are effected.

- CSCdp91476

  The fix for this DDTS adds a 32-bit overflow counter that can be used in conjunction with the existing 32-bit counter to get the full 64-bit value. In addition, a true 64-bit counter has also been added to the MIB. SNMP v1 managers and Cisco IOS Release 11.X releases are limited to using the 32-bit overflow counters; the 64-bit counters will be invisible to them. SNMP v2 and SNMP v3 managers that are running on top of Cisco IOS Release 12.X releases will be able to use either the 32-bit overflow counters or the 64-bit counters.

- CSCdr01116

  A Cisco 12000 Gigabit Switch Router (GSR) that is configured for 802.1Q trunking over a Gigabit Ethernet interface might not form OSPF or EIGRP adjacencies when **ip route-cache flow** is configured on the main Gigabit Ethernet interface.

  Workaround: Configure and use Gigabit Ethernet subinterfaces or disable flow switching by entering the **no ip route-cache flow** command.

TCP/IP Host-Mode Services

- CSCdp63037

  Border Gateway Protocol (BGP) sessions on Cisco 12000 series Gigabit Switch Router (GSR) might fail to send updates when the router establishes passive BGP sessions because of problems with the flow control of BGP and TCP.

  Workaround: Use an inbound Access Control List (ACL) to deny any traffic destined for the port, and always open the session actively.

Wide-Area Networking

- CSCdp51767

  A Cisco 7500 series Route Switch Processor (RSP) with a VIP2-50 Versatile Interface Processor and a PA-A3 port adapter might not react to available bit rate (ABR) explicit rate (ER) congestion marking. In this situation, the output rate of an ABR connection does not decrease upon the reception of a Resource Management (RM) cell with an ER field value that is lower than the CCR value. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(9)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(9)S. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdm81049

  If a serial interface is flapping up and down repeatedly, the router might pause indefinitely with a stack trace indicating that it is in usecdelay() as a result of cbus_mci_serial_reset() being called while at interrupt level. This situation rarely occurs.

  Workaround: Enter the **shutdown** interface configuration command on the serial interace that is flapping up and down.

- CSCdp23786

  A Cisco router that is running Cisco IOS Release 12.0(7)T cannot execute boot configuration commands from Flash, and exhibits the following error message:

  ```
  %Error opening nvram:/startup-config (File system is in an inconsistent state)
  ```

  When this message is displayed, no configuration is loaded. If you enter the **copy startup-config running-config** command and then enter the **no shutdown** interface configuration command, the router will come back on line. There is no workaround.

- CSCdp56057

  Cisco 3620 routers and Cisco 3640 routers might exhibit traceback messages after being reloaded. The tracebacks occur because of uninitialized semaphore attempts to become locked. This situation does not affect the router functions. There is no workaround.

- CSCdp57908

  This caveat adds support for a new revision of a hardware component that fixes a previous error. For the benefit of users that have not upgraded to the new hardware, it will also exhibit a warning error message that indicates the old hardware revision.

  Cisco 7200 series routers with NPE-175 or NPE-225 network processing engines must upgrade to Cisco IOS releases that incorporate this change (for example, Cisco IOS Release 12.0(9) and later releases or Cisco IOS Release 12.0(9)S and later releases). Use of older Cisco IOS releases might result in unpredictable malfunctions. Please see the following document for further information:

  http://www.cisco.com/warp/customer/770/fn8611.shtml

IBM Connectivity

- CSCdp09919

  Remote source-route bridging (RSRB) might change frame types. This situation occurs on Cisco routers that are running RSRB where one side of the RSRB is running Cisco IOS Release 11.0 and the other side is running Cisco IOS Release 12.0. The frame that is moving along the source-route translational bridging (SR/TLB) and RSRB bridge will be changed from an Ethernet Type II frame to an IEEE 802.3 Ethernet frame.

  Workaround: Configure the 90-compatible option by entering the **source-bridge transparent** *ring-group pseudo-ring bridge-number tb-group* [*90-compatible*] global configuration command.

Interfaces and Bridging

- CSCdm19573

  A Cisco 7200 series router that is running Cisco IOS Release 11.1(22)CC or Cisco IOS Release 11.1(25)CC with a PA-CT3 might experience problems with local-area transport (LAT) services under the following conditions:

  If you are using transparent bridging with LAT enabled on a serial interface, you might not see LAT services when entering the **show lat service** command, even when the remote link (also using transparent bridging with LAT enabled) is advertising LAT services. There is no workaround.

- CSCdp18313

  A Cisco 7206VXR router that is running Cisco IOS Release 12.0(6.5)T2 and has a network processing engine (NPE)-300 network processing engine might reload with a bus error. There is no workaround.

IP Routing Protocols

- CSCdp26552

  Open Shortest Path First (OSPF) and summary link-state advertisement (LSA) is not installed in the routing table.

  Workaround: Clear the routing table and restart the OSPF process.

- CSCdp30454

  The dataless header register is not working properly in Cisco IOS Release 12.0(7)S. There is no workaround.

- CSCdp39843

  If a Cisco router receives a Resource Reservation Protocol Reserve (RESV) message to refresh a label-switched path (LSP) for which it is the source, and if the RESV message contains a Multiprotocol Label Switching (MPLS) label other than the one previously received, the router will attempt to perform a label change operation. If the label change operation fails, the router might reload while executing the appropriate error handling procedures. This situation rarely occurs. There is no workaround.

- CSCdp57762

  A Cisco router that is running Cisco IOS Release 12.0(05.06)S03 or later releases up to Cisco IOS Release 12.0(8.5)S might not send withdraw requests and not delete the entry from the IP routing table under the following *SOFT RESET* conditions:

  – The **neighbor soft-reconfiguration** router configuration command is entered on the router for a particular peer.

  – The **route-map** global configuration command is entered to modify attributes.

  – There is a used entry and a received-only entry for a given prefix, and the **neighbor filter-list**, **neighbor distribute-list**, or **neighbor prefix-list** router configuration commands or the **route-map** global configuration command is entered to deny this prefix.

  – The **soft clear bgp** EXEC command is entered.

  Symptoms of this situation include the prefix being present in the Border Gateway Protocol (BGP) table with the received-only path, the prefix remaining in the IP table, and the prefix not being withdrawn from all the other peers to which it has advertised. These symptoms do not occur if both

peers are route-refresh capable, soft-reconfiguration inbound is not configured, the filter that you apply does not result in a deny for a prefix, if you do a hard reset, or the soft reconfiguration is done through route-refresh.

Workaround: If you have soft cleared the session after applying the filter, enter the **clear ip bgp** {*} [**soft out**] EXEC command.

Alternate workaround: Upgrade to Cisco IOS Release 12.0(8.5)S.

Miscellaneous

- CSCdk77704

  If you enable fancy queueing on an interface where it is the default, the queueing behavior might not function properly. There is no workaround.

- CSCdp17433

  The Forwarding Information Base (FIB) scanner might not free a locked FIB entry so the FIB path chunks will never be freed, resulting in a memory leak. There is no workaround.

- CSCdp35794

  When Access Control Lists (ACLs) are used, Gigabit and Fast Ethernet line cards might experience data corruption. This situation is likely to happen for non-Address Resolution Protocol (ARP) standard Ethernet style (RFC 826) encapsulation packets.

  When extended or compiled ACLs are used, a Gigabit Switch Router (GSR) with Gigabit Ethernet (GE) or Fast Ethernet (FE) line cards might experience line-card failures or corruption of internal queueing structures. This failure might result in incorrect traffic forwarding behavior for packets received on affected cards.

  This failure will not occur if ACLs are not used. Even when ACLs are configured, the occurrence of this failure is still rare. Conditions that will increase the frequency of the error occurring are the use of compiled access lists, large amounts of traffic with nonstandard Ethernet encapsulations, or the presence of large amounts of ARP traffic.

  Workaround: Reset the card by entering the **microcode reload** [*slot-number*] global configuration command.

- CSCdp38982

  When a first label switch router (LSR) is sending Multiprotocol Label Switching (MPLS) encapsulated IP frames to a second LSR that is removing the last label and sending the resultant IP frame onto an Inter-Switch Link (ISL), then IP packets of less than 44 bytes will be received as cyclic redundancy check (CRC) errors. There is no workaround.

- CSCdp41376

  Multiprotocol Label Switching (MPLS) imposition load balancing adjacency entry updates might cause the Gigabit Switch Router (GSR) performance line cards to reload. There is no workaround.

- CSCdp42529

  A Cisco 7200 VXR router might experience a situation where switched virtual circuits (SVCs) are disconnected intermittently and then recovered after 7 to 20 hours. There is no workaround.

- CSCdp46780

  After the primary clock scheduler card (CSC) has been removed, a Cisco OC-48/STM-16 Packet-over-SONET/SDH line card might not recover from being switched to the secondary CSC card and report error messages.

  Workaround: Reload the line card.

- CSCdp47676

  Under certain timing conditions on some Versatile Interface Processors (VIPs), 2-port High-Speed Serial Interfaces (HSSIs) or PA-2T3s might experience abnormal transmit underruns as indicated by the **show interfaces** EXEC command. There is no workaround.

- CSCdp52926

  Output committed access rate (CAR) might not function properly when running on a non-Versatile Interface Processor (VIP) interface. Traffic does not pass properly through the output interface that is enabled with CAR. There is no workaround.

- CSCdp54813

  A Cisco 7500 series router will often reload when switching onto an IP tunnel if sending to the tunnel destination involves Multiprotocol Label Switching (MPLS) label imposition. There is no workaround.

- CSCdp58615

  A Versatile Interface Processor (VIP) might reload after distributed committed access rate (DCAR) is configured and traffic is present on the VIP interface. The condition returns to normal after the VIP reloads. There is no workaround.

- CSCdp58675

  Received packets that had been padded by the previous hop are corrupted by the Multiprotocol Label Switching (MPLS) distributed Cisco Express Forwarding (dCEF) label imposition code, which will result in IP checksum errors at their final destination or at an intermediate hop, depending on the network configuration.

  Workaround: Disable dCEF globally or on a per-VIP interface basis.

- CSCdp64140

  Two Cisco 12000 series Gigabit Switch Routers (GSRs) that are connected by a Gigabit Ethernet (GigE) connection might exhibit “GRP-4-CORRUPT” error messages when one of the routers is upgraded to Cisco IOS Release 12.0(8)S. There is no workaround.

Wide-Area Networking

- CSCdm56380

  When an ATM switch is not configured, a permanent virtual circuit (PVC) or one of the subinterfaces might be shut down on the other side of the ATM switch, but the Simple Network Management Protocol (SNMP) agent reflects that the subinterface shows the subinterface as being UP(AdminStatus and OperStatus). There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(8)S

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(8)S. This section describes only severity 1 and 2 caveats.

IP Routing Protocols

- CSCdp15126

  If you enable policy routing on a Fast Ethernet Inter-Switch Link subinterface, the packet that is destined for the next hop is not policy routed. Instead, the packet is sent along the default route. There is no workaround.

Miscellaneous

- CSCdm36033

  The **pos delay triggers line** command is used for GSR POS interfaces connected to internally-protected DWDM systems. This command is invalid for interfaces that are configured as APS working or protected. Normally, even a few microseconds of line- or section-level alarms (SLOS, SLOF, or LAIS) will bring down the link until the alarm has been clear for ten seconds. If holdoff is configured, this link-down trigger is delayed for 100 ms. If the alarm stays up for more than 100 ms, the link is brought down as it is now. If the alarm clears before 100 ms, the link is not brought down.

- CSCdm82546

  The Gigabit Switch Router (GSR) Performance line cards do not have the ability to load balance between IP and tag adjacencies. There is no workaround.

- CSCdp05571

  Entering the **show access-list** [#] command will report statistics for matches to fast Access Control List (ACL) items. Statistics are reported on an item by item basis and appear in parenthesis to right of the item. The statistics reported represent the running sum of matches to the item on all interfaces. This new command output fixes the problem of statistics for ACLs not being displayed in previous releases.

- CSCdp10843

  When disabling distributed Cisco Express Forwarding (dCEF) on a running system, clean up all forwarding entries on the line card and move all incoming packets to the Route Processor (RP). The intent is to leave line card forwarding in the state it would have been in if dCEF had never been enabled in the first place.

  Midpoints for Multiprotocol Label Switching traffic engineering (MPLS-TE) tunnel link-state packets (LSPs) do not get cleaned up when dCEF is disabled so when packets arrive at a Versatile Interface Processor (VIP) with the MPLS labels for these stale midpoint entries, the VIP will not forward these packets correctly.

  Workaround: Reload any line card on which dCEF has been disabled if that line card is, or might be at some point, an incoming interface for an MPLS-TE tunnel LSP.

- CSCdp21343

  Some permanent virtual connections (PVCs) in ATM line cards do not function. The **show atm vc** command indicates that the ATM PVC peak and average rates are zero. The state of any sub-interfaces remain INACTIVE. During a reload when the shut ATM sub-interface is encountered, all subsequent sub-interfaces within that interface will be ignored.

  Workaround: Ensure that the ATM interface is not shut. Enter the **shut** and **no shut** commands on each affected ATM sub-interface.

- CSCdp21424

  Under certain conditions, a Cisco 7200 or 7500 series router with a multichannel E1/T1 port adapter might exhibit the following error message:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=Serial3/0:0
  ```

  There is no workaround.

- CSCdp31259

  Enhanced OC48 Packet-Over-SONET (POS) line cards will not boot correctly if the fabric downloader is upgraded while running affected images. This problem can be triggered by the following commands:

Command	Mode
service upgrade all	configuration
upgrade all all	enabled EXEC
upgrade fabric-downloader all	enabled EXEC
upgrade fabric-downloader [*slot#*]	enabled EXEC

  The problem causes the line card to boot incorrectly. Changing to a different version of code is required to correctly load the card once the fabric downloader upgrade has been executed. The upgrade will need to be reinstalled after reload.

  Workaround: Do not upgrade the fabric downloader by avoiding the upgrade commands.

- CSCdp31471

  The available bit rate (ABR) feature on PA-A3 does not work. The PA-A3 driver can send and receive forward resource management (FRM) cells but backward resource management (BRM) cells cannot be transmitted. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(7)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(7)S. This section describes only severity 1 and 2 caveats.

IBM Connectivity

- CSCdm89688

  A Cisco 7000 series router with two CIP cards that are both running **tn3270-server** might unexpectedly reload with a software forced crash if you remove the **client ip** configuration command. There is no workaround.

Miscellaneous

- CSCdm70554

  A Gigabit EtherChannel (GigE) line card might pause indefinitely in FABL START state when the secondary Gigabit Route Processor (GSR) is in the chassis.

  Workaround: Remove the secondary Gigabit Route Processor (GSR).

- CSCdm72149

  When formatting a PCMCIA card with Cisco IOS Release 12.0 S, the command might fail if you have not formatted your bootflash.

  Workaround: Format your bootflash and try the operation again.

- CSCdm74152

  A Cisco router that is running Cisco IOS Release 12.0(4.6)T through 12.0(5)T might experience problems with fast switching if Cisco Express Forwarding (CEF) is disabled.

  Workaround: Enable Cisco Express Forwarding (CEF), and then disable CEF to remove it from the unwanted interfaces.

- CSCdm77266

  A Cisco 12000 router that is running the "gsr-k4-p" software image in Cisco IOS Release 12.0(5.5)S2 might reload if you simultaneously configure Border Gateway Protocol (BGP) neighbors and static routes and Multicast Source Discovery Protocol (MSDP). There is no workaround.

- CSCdm89160

  After you upgrade the ROM monitor on a Cisco router, the router might not reload properly and exhibit the following error message:

  ```
  *** Cache Error Exception *** Cache Err Reg = 0xa4240560 data reference, primary
  cache, data field error , error on SysAD Bus PC = 0xbfc00e04, Cause = 0x8000,
  Status Reg = 0x30408404 Tiger Masked Interrupt Register = 0x000000ff Tiger
  Interrupt Value Register = 0x0000000c
  ```

  This situation occurs only when the following conditions exist:

  1) The router is running one of the following IOS software images: 11.2(17)GS1; 12.0(5.5)S1 and later versions prior to this fix; 12.0(5.6)S and later versions prior to this fix; or 12.0(6.0.2)S and later versions prior to this fix.

  2) You have manually upgraded the ROM monitor using either the **upgrade rom slot** [**RP-slot#**] command or the **upgrade all all** command. If you used the **upgrade all all** command, answering "yes" when prompted to upgrade the Route Processor (RP) ROM monitor will cause this situation to occur.

  Workaround: Do not upgrade the ROM monitor.

- CSCdp00618

  A Route/Switch Processor (RSP) might reload while unprovisioning a channelized interface under heavy traffic. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(6)S

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(6)S. This section describes only severity 1 and 2 caveats.

IP Routing Protocols

- CSCdk70273

  If there are more than 31 OSPF interfaces, flooding does not work, starting from the 32nd OSPF interface. There is no workaround.

- CSCdm34431

  An RSP4 Route/Switch Processor that is running Cisco IOS Release 12.0(3.6)T or 12.0(4)T might reload with the following error message if you issue the **copy tftp running** command to update the configuration while the Versatile Interface Processor (VIP) or Route/Switch Processor (RSP) is under a heavy traffic load:

  ```
  ipfib_policy_forward vip_ip_fib_flow amdfe_rx_interrupt s_amdfe_check
  ```

  This situation occurs when the RSP is running with a VIP2-50 Versatile Interface Processor, a Fast Ethernet port adaptor, and PA-A3 and is configured with distributed Cisco Express Fowarding (dCEF), policy routing, and NetFlow.

  Workaround: Avoid reloading the configuration with the **copy tftp running** command.

- CSCdm51092

  A Cisco router might reload if you enter the same **no ip msdp mesh-group** *foo peer-address* command twice. There is no workaround.

- CSCdm59659

  When “debug ip icmp” is enabled on a line card in a Cisco 12000 series Gigabit Switch Router (GSR), it cannot be disabled. There is no workaround.

- CSCdm60244

  A Cisco router might reload if you perform a router_id change or issue the **clear ip bgp** {*****} command when Multicast Border Gateway Protocol (MBGP) is enabled.

  Workaround: Avoid issuing the **clear ip bgp** {*****} command or changing router_id.

- CSCdm94032

  Border Gateway Protocol (BGP) routes might not be withdrawn if deterministic med is not enabled.

  Workaround: Configure deterministic med by issuing the **bgp deterministic med** command.

ISO CLNS

- CSCdm61381

  A Cisco 2500 series router might reload if you issue the **no router isis** [*tag*] command. There is no workaround.

Miscellaneous

- CSCdm09656

  After you load the image on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S and Release 12.0 T, issuing the **no shutdown** command on a T1 controller that is up causes the T1 controller to go down. Channels created under that controller also go down. This only happens with T1 and does not occur on Cisco 7200 series routers.

  Workaround: Issue the **shutdown** command followed by the **no shutdown** command on the T1 controller. If this fails, perform a microcode reload to bring the controller back up.

- CSCdm12259

  The rate limit on a Gigabit Switch Router (GSR) might not work properly if input Committed Access Rate (CAR) based on QoS groups is configured. There is no workaround.

- CSCdm66427

  If you use the "log" keyword in an Access Control List (ACL) that is used to filter routes, it might result in alignment errors that cause increased CPU utilization and interfere with normal router operation.

  Workaround: Remove the "log" keyword from the configuration.

Wide-Area Networking

- CSCdm49871

  A Cisco router reloads when you deconfigure a routing protocol (for example, when you issue the **no ipx routing** command). The problem exists in Cisco IOS Release 12.0(3)T and Release 12.0(3)S and later releases. At least one Frame Relay interface must be configured and at least one Frame Relay map (an association between a DLCI and a level 3 protocol address) must be established by Inverse ARP.

  Workaround:

  (a) Disable Inverse ARP for the routing protocol to be deconfigured (for example, for IPX routing, use the **no frame-relay inverse-arp ipx** *dlci* interface configuration command).

  (b) Clear the Frame Relay Inverse ARP cache using the **clear frame-relay-inarp** executive command.

  (c) Remove the routing protocol from the router (for example, for IPX routing, use the **no ipx routing** global configuration command).

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family and Cisco 12000 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents except for feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with these documents:

Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

  On CCO at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on CCO at:

  Technical Documents

- Caveats for Cisco IOS Release 12.0

  As a supplement to the caveats listed in the "Caveats" section in these release notes, see *Caveats for Cisco IOS Release 12.0*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0.

  On CCO at:

  Technical Documents: Documentation Home Page: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **Caveats**

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Service & Support: Online Technical Support: Software Bug Toolkit**, or at http://www.cisco.com/support/bugtools.

Platform-Specific Documents

These documents are available for the Cisco 7000 family and Cisco 12000 series routers on CCO and the Documentation CD-ROM:

- Installation and Configuration Guides and Configuration Notes
- User Guides
- Hardware Installation and Maintenance Guides
- Regulatory Compliance and Safety Documentation

On CCO at:

Technical Documents: Documentation Home Page: Core/High-End Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Core/High-End Routers

Feature Modules

Feature modules describe new features supported by Release 12.0 S and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **New Feature Documentation: New Features in 12.0-Based Limited Lifetime Releases: New Features in Release 12.0 S**

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.0**: **New Feature Documentation: New Features in 12.0-Based Limited Lifetime Releases: New Features in Release 12.0 S**

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command reference publications, and several other supporting documents, which are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On CCO and the Documentation CD-ROM, two master documents provide information for the Cisco IOS software documentation set.

You can reach these documents on CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

You can reach these documents on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

Note You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

You can reach the Cisco IOS documentation set on CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 8 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
• *Configuration Fundamentals Configuration Guide* • *Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
• *Bridging and IBM Networking Configuration Guide* • *Bridging and IBM Networking Command Reference*	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set

Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Dial Solutions Configuration Guide* • *Dial Solutions Command Reference*	X.25 over ISDN AppleTalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 and T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles Dial-Out Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
• *Network Protocols Configuration Guide, Part 1* • *Network Protocols Command Reference, Part 1*	IP Overview IP Addressing and Services IP Routing Protocols
• *Network Protocols Configuration Guide, Part 2* • *Network Protocols Command Reference, Part 2*	AppleTalk Novell IPX
• *Network Protocols Configuration Guide, Part 3* • *Network Protocols Command Reference, Part 3*	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Security Configuration Guide* • *Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
• *Wide-Area Networking Configuration Guide* • *Wide-Area Networking Command Reference*	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
• *Voice, Video, and Home Applications Configuration Guide* • *Voice, Video, and Home Applications Command Reference*	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
• *Quality of Service Solutions Configuration Guide* • *Quality of Service Solutions Command Reference*	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signalling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
• *Cisco IOS Software Command Summary* • *Dial Solutions Quick Configuration Guide* • *System Error Messages* • *Debug Command Reference*	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**.

Obtaining Documentation

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.